AS Sertifitseerimiskeskus

DigiDocService spetsifikatsioon

Dokumendi versioon: 3.8.1
Viimati uuendatud 09.03.2015
Kirjeldatav teenuse versioon: 3.8.1

Sisukord

1 Dokumendi muudatuste ajalugu 3
2 Viited 7
3 Mõisted 7
4 Sissejuhatus 8
4.1 Digitaalallkirjade vormingud 9
4.1.1 DDOC vorming 9
4.1.2 BDOC vorming 10
4.2 Signeerimise algoritmid 10
5 Nõuded ja soovitused rakenduse pakkujale 11
5.1 Nõuded digitaalallkirjastamisele 11
5.2 Nõuded Mobiil-ID toimingute käivitamiseks 11
5.3 Tehnilised nõuded ja soovitused 12
6 Peamised kasutusjuhud 13
6.1 Allkirjastatud faili verifitseerimine 13
6.2 Allkirjastamine 14
6.2.1 Mobiiliga Allkirjastamine asünkroonselt Client-Server režiimis 14
6.2.2 Kiipkaardiga allkirjastamine 16
6.3 Autentimine 18
6.3.1 Mobiil-ID autentimine asünkroonselt klient-server režiimis 18
6.3.2 Kiipkaardiga autentimine 19
7 Autentimisega seotud teenuse päringud ja vastused 19
7.1 MobileAuthenticate 19
7.2 GetMobileAuthenticateStatus 22
7.3 CheckCertificate 24
8 Digitaalallkirjastamisega seotud teenuse meetodid 25
8.1 StartSession 25
8.1.1 HASHCODE kuju 26
8.1.1.1 BDOC vorming ja HASHCODE 27
8.1.1.1.1 BDOC konteineri HASCODE kujule teisendamine 27
8.1.1.1.2 BDOC konteineri teisendamine tagasi standardkujule 28
8.1.1.2 DigiDoc (DDOC) vorming ja HASHCODE 29
8.2 CloseSession 31
8.3 CreateSignedDoc 31
8.4 AddDataFile 32
8.5 MobileSign 33
8.6 GetStatusInfo 36
8.7 GetSignedDocInfo 37
8.8 GetSignedDoc 38
8.9 GetDataFile 38
8.10 RemoveDataFile 39
8.11 RemoveSignature 39
8.12 GetSignersCertificate 40
8.13 GetNotarysCertificate 41
8.14 GetNotary 41
8.15 GetVersion 42
8.16 PrepareSignature 42
8.17 FinalizeSignature 44
8.18 MobileCreateSignature 44
8.19 GetMobileCreateSignatureStatus 48
8.20 GetMobileCertificate 49
8.21 MobileSignHashRequest 50
8.22 GetMobileSignHashStatusRequest 51
9 Kasutatavad andmestruktuurid 53

9.1 SignedDocInfo 53
9.2 CertificateInfo 56
9.3 DataFileInfo 57
9.4 SOAP veakoodid 57
9.5 Konteineri valideerimine 59
10 Teenuse muudatuste ajalugu 60

1 Dokumendi muudatuste ajalugu

Ver.	Kuupäev	Muutja	Täiendused
3.8.1	09.03.2015	Risto Alas	- Meetodile „MobileCreateSignature“ on lisandunud tugi formaadile BDOC-TS ehk ASiC-E. Viimase kasutamiseks tuleb seada „SigningProfile“-parameetri väärtuseks „LT“. - Mobiil-ID toimingutele lisatud info sessiooni aegumise aja kohta
3.7.1	08.12.2014	Risto Alas	- Uuendatud allkirjastamisalgoritmide peatükki (4.2). Teenus toetab Mobiil-ID SIM-kaarti, mis kasutab mitut allkirjastamisalgoritmi (nt RSA ja ECDSA) korraga ühe SIM-kaardi peal). - Täiendatud ECDSA autentimisallkirjade verifitseerimise kirjeldust (peatükk „GetMobileAuthenticateStatus()”). - “SigningProfile”- parameetrile on defineeritud uus reserveeritud väärtus “LT” (ingl k *Long Term*, nimetus pärineb ASiC-standardist). Antud väärtust kasutatakse teenuse järgmises versioonis BDOC-TS (BDOC ajatempliga ehk ASiC-E) formaadi tähistamiseks, hetkel tagastab teenus vea.
3.6	25.08.2014	Risto Alas, Priit Reiser	- Lisatud HASHCODE kuju kasutamise kirjeldus BDOC-formaadile - MobileCreateSignature-meetodile lisandus mittekohustuslik atribuut "MimeType" - Parandatud andmefaili sisu tüüpi peatükis 9.3 (DataFileInfo).
2.128	17.04.14	Tauri Neitov	- Täpsustatud StartSession() ja MobileCreateSignature() meetodite kirjeldusi - Muudetud konteineri valideerimise infot
2.127	26.03.14	Tauri Neitov	- Täpsustatud BDOC versiooni 2.1 tuge - Lisatud peatükk DigiDoc teegi veateadete edastamise kohta - Täiendatud GetMobileCertificate() meetodi vastuse kirjeldust - Kirjeldatud ECDSA sertifikaatide tugi GetMobileAuthenticateStatus() meetodi vastuses

2.126	16.01.14	Ago Vesmes, Tauri Neitov	- Korrigeeritud teksti - Täiendatud meetodite MobileAuthenticate(), MobileCreateSignature(), MobileSign() ja GetMobileCertificate() kirjeldusi riigi välja kohustuslikkuse osas. - Lisatud meetodite MobileSignHashRequest() ja GetMobileSignHashStatusRequest() kirjeldused. - Täiendatud SOAP veateadete kirjeldusi. - Parandatud muutuja nimi MobileAuthenticate() meetodi sisendis. - Täiendatud lubatud konteinerite formaatide ja versioonide loetelu - Teenuse muudatuste loetelu eemaldatud ja viidud id.ee veebi. - Eemaldatud peatükid DigiDocist, DigiDoci turvamudel ja GetSignatureModules.
2.125	18.03.13	Ahto Jaago, Liisa Lukin, Ago Vesmes	- Täiendatud meetodite MobileAuthenticate(), MobileSign(), MobileCreateSignature() ja GetMobileCertificate() kirjeldusi isikukoodi ja telefoninumbri väljade kohustuslikkuse osas. Lisandus võimalus kasutada nende meetodite puhul, kus on Language väli, väärtust „LIT“. Samuti täpsustus lisainfovälja (MessageToDisplay) pikkus - Muudetud ja täiendatud nõudeid Mobiil-ID toimingute käivitamisel - Täiendatud ja parandatud meetodi StartSession() kirjeldust - Allkirjastamisel ja konteineri loomisel on toetatud ainult DIGIDOC 1.3 konteineri formaat. - Täiendatud ja parandatud meetodite MobileCreateSignature() ja CreateSignedDoc() kirjeldust. - Täiendatud ja parandatud meetodi GetMobileCreateSignatureStatus() kirjeldust - Täiendatud peatükke 6.2.2 Kiipkaardiga allkirjastamine, – lisatud soovitus GetSignatureModules meetodi asemel kasutada idCard.js klienditeeki - Täiendatud punkte 5.3, 8.1, 8.4 ja 8.18 infoga DigiDocService-isse saadetavate failide mahupiirangust ning HASHCODE kujul andmete saatmisest teenusesse. - Täiendatud tagastatavate veakoodide kirjeldusi peatükkides 9.4, 8.6, 8.23 - Lisatud teenuse versioonide 2.3.5 ja 3.2.5

			erinevuste kirjeldus
2.123	19.12.08	Ahto Jaago, Urmo Keskel	- Lisatud peatükk „Nõuded ja soovitused teenuse kasutamisel“ - Lisatud meetodi CheckCertificate kirjeldus - Lisatud punkt Kiipkaardiga autentimine - Täiendatud kirjeldusi meetodite StartSession, MobileAuthenticate, MobileAuthenticateStatus, AddDataFile ning andmestruktuuri DataFileInfo juures - Parandatud punkti 6.2.1 juures olevat joonist ja tegevuste kirjeldusi
2.122	23.04.07	Urmo Keskel	- Lisatud GetMobileCertificate meetodi kirjeldus. - Korrigeeritud teksti.
2.120	02.03.07	Urmo Keskel	- Lisatud täiendavad staatused meetodi GetMobileAuthenticateStatus ja GetStatusInfo vastustesse. - Täiendatud SOAP veakoodide loetelu. - Parameetrite nimetused nüüd kõikjal suure algustähega (Sesscode, Status, jne). - DataFileAttribute ja DataFileInfo->Attributes elementide nimetused viidud keeleliselt korrektseteks.
2.112	13.02.07	Urmo Keskel	- Muudetud asünkroonset tagasisaatmist - Lisatud WaitSignature parameetrid meetoditele GetMobileAuthenticateStatus ja GetStatusInfo. - Lisatud ChallangeID MobileSign ja - MobileCreateSignature meetodite vastustele. - Lisatud SOAP veakoodide esialgsed kirjeldused. - Lisatud ServiceName parameeter MobileSign meetodile.
2.110	22.01.07	Urmo Keskel	Muudetud MobileCreateSignature päringu kirjeldust (FileInfo elemendile lisatud DigestType parameeter, lisatud failiversiooni parameeter), asynchServerServer režiim viidud kaheks: asynchServerServerJMS ja asynchServerServerSOAP.
2.109	13.12.06	Urmo Keskel	- Kirjeldatud asynchServerServer režiimis vastuste saatmine; - Lisatud meetodite MobileCreateSignature ja GetMobileCreateSignatureStatus kirjeldused.
2.108	24.11.06	Urmo Keskel	Pisimuudatused GetMobileAuthenticateStatus päringu kirjelduses
2.107	16.10.06	Urmo Keskel	- Mobiilautentimise ja isikutuvastuse päringutele lisatud riigi kood; GetMobileAuthenticateStatus lisatud parameeter WaitSignature;

			- MobileAuthenticate päringule lisatud parameeter ServiceName; - MobileAuthenticate meetodi MessageToDisplay parameeter nüüd mittekohustuslik.
2.006	26.05.06	Urmo Keskel	Kirjeldatud mobiilautentimise päringud ja lisatud mobiiliga isikutuvastuse toimingu jadadiagramm.
2.005	03.05.06	Urmo Keskel	Muudetud meetodeid StartSession ja MobileSign, lisatud signatureProfile parameeter. Lisatud ajatempleid ja tühisusnimekirju puudutavad meetodid. Dokumentatsioonist eemaldatud näitepäringud.
2.004	10.11.05	Urmo Keskel	GetSignedDocInfo päringu viidud teenuse versioonis 1.000 olnud kujule, lisatud meetodi GetStatusInfo kirjeldus. Lisatud peatükk “Teenuse muudatuste ajalugu”.
2.003	31.10.05	Urmo Keskel	Esimene versioon, baseerub Veiko Sinivee koostatud dokumendil “DigiDocService teenuse mudel ja spetsifikatsioon”

2 Viited

	Viide
[1] RFC3275	(Extensible Markup Language) XML-Signature Syntax and Processing. March 2002.
[2] ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES). February 2002.
[3] DigiDoc vorming	http://www.id.ee/28737
[4] SOAP	Simple Object Access Protocol http://www.w3.org/TR/soap/
[5] Time Formats	The W3C note Date and Time Formats *http://www.w3.org/TR/NOTE-datetime*, September 1997
[6] ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface. V.1.1.4, August 2003.
[7] RFC 3161	Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP), August 2001
[8] NIST P-256	National Institute of Standards and Technology poolt soovitatud elliptilise krüptograafia kurv. http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf
[9] BDOC formaadi spetsifikatsioon	http://sk.ee/repository/bdoc-spec21.pdf
[10] XMLDSIG (XML allkirjade süntaks ja töötlemine)	http://www.w3.org/TR/xmldsig-core1/

3 Mõisted

Mõiste	Kirjeldus
Algfail, Andmefail	Suvalises vormingus andmefail, mida hakatakse allkirjastama.
Allkirjastamine	Tekstis käsitletud kui „digitaalse allkirja moodustamine Digitaalallkirja Seaduse mõistes“. Toiming sisaldab lisaks signeerimisele kehtivuskinnituse võtmist
Kontrollkood	Mobiil-ID’ga allkirjastamisel ja autentimisel kasutatav neljakohaline number, mis krüptograafiliselt seotud allkirjastava räsiga. Kontrollkood kuvatakse nii allkirjastamist/autentimist võimaldavas rakenduses kui telefoni ekraanil, võimaldamaks kasutajal veenduda allkirjastamise / autentimispäringu autentsuses.
MSSP	Mobile Signature Service Provider – mobiilallkirjastamise teenuse pakkuja. Kirjeldatud standardis ETSI TS 102 204 [6].

Mõiste	Kirjeldus
Mobiil-ID	ID-kaardiga analoogiline autentimise ja digitaalallkirjastamise teenus. Mobiil-ID kasutaja omab spetsiaalset SIM kaarti, millel on kasutaja salajased võtmed. Autentimisel või allkirjastamisel edastatakse signeeritav räsi üle mobiilivõrgu telefoni ja kasutaja peab tehingu teostamiseks sisestama telefoni autentimise/allkirjastamise PIN koodi. Signeerimise järgselt saadetakse tekkinud tulem teenusesse.
Rakenduse pakkuja	DigiDocService teenuse tarbija, pakub kasutajale allkirjastamist, allkirjade verifitseerimist või autentimist võimaldavat rakendust.
Räsi, Räsikood	Signeeritav andmehulk, mis on krüptograafiliselt seotud allkirjastatavate algfailide ja muude allkirja parameetritega
Signeerimine	Privaatvõtme rakendamine lähtetekstile. Tulemuseks on „signatuur“.
Teenuse pakkuja	DigiDocService teenuse pakkuja.
Verifitseerimine	Digitaalallkirjastatud andmekogumi allkirja(de) kontroll.

4 Sissejuhatus

DigiDocService on SOAP põhine veebiteenus võimaldamaks võimalikult lihtsalt autentimise, digitaalallkirjastamise ja allkirjade verifitseerimise funktsionaalsust siduda teiste infosüsteemidega.

Teenust on võimalik kasutada erinevatelt arenduskeskkondadest/platvormidelt, millel on SOAP 1.0 RPC-encoded tugi.

Teenuse poolt pakutav funktsionaalsus:

- Isikusamasuse kontroll Mobiil-ID’ga
- Sertifikaatide kehtivuse kontroll (isikusamasuse kontroll ID-kaardi ja muu kiipkaardiga)
- DigiDoc/BDOC failide moodustamine
- DigiDoc/BDOC digitaalallkirjastamine Mobiil-ID’ga
- DigiDoc/BDOC digitaalallkirjastamine ID-kaardi (ja muu kiipkaardiga)
- Digitaalallkirjastatud failide (DigiDoc/BDOC) sisu ja allkirjade kehtivuse kontroll
- Räsi allkirjastamine Mobiil-ID’ga

Teenusele ligipääsu võimaldatakse IP aadressi põhiselt, teenuse kasutamiseks tuleb rakenduse pakkujal sõlmida leping AS Sertifitseerimiskeskusega, teenuse kasutamise maksumus sõltub allkirjastamise ja autentimise päringute arvust kuus ja ühelt rakenduselt tulevatest üheaegsete päringute arvust.

DigiDocService toetab digiallkirjastatud dokumendikonteineri DIGIDOC-XML 1.3 ja BDOC 2.1 ajamärgendiga *(time-marking)* failivormingut. BDOC ajatempliga (*timestamp*) formaadi tugi on versioonis 3.8 vaid MobileCreateSignature meetodi

kasutamisel, ülejäänud teenuse meetoditele lisandub ajatemplitega BDOC formaadi tugi teenuse versioonis 3.9

Vanemate formaatide puhul (SK-XML 1.0, DIGIDOC-XML 1.1 ja DIGIDOC-XML 1.2) on toetatud ainult allkirja verifitseerimine (dokumendi konteineri formaati kontrollitakse MobileCreateSignature ja CreateSignedDoc meetodites, kus ebasobiva kombinatsiooni korral tagastatakse SOAP veaobjekt teatega 'Invalid format and version combination')

4.1 Digitaalallkirjade vormingud

4.1.1 DDOC vorming

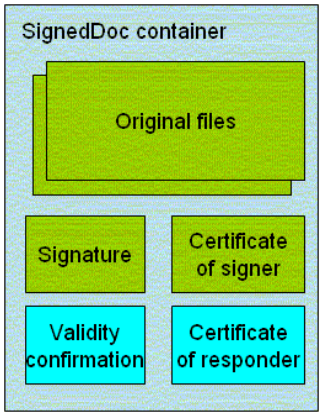
Digitaalallkirjastatud failide formaat baseerub ETSI TS 101 903 standardile, mida kutsutakse "XML Advanced Electronic Signatures (XAdES)". Antud standard kirjeldab digitaalallkirjastatud dokumentide struktuuri erinevatel täiendava kehtivuskinnituse info sisalduvuse tasemetel .

Võttes aluseks ülaltoodud usaldusmudeli, vastab DigiDoc XAdES profiilile "XAdES-X-L"-ile, kuid RFC 3161 ajatemplite asemel kasutatakse nn "ajamärgist" (allkirjastamise ametlik aeg on fikseeritud OCSP kehtivuskinnituse ajaga).

Antud profiil:

- Võimaldab allkirjaga siduda järgnevad allkirjastatavad atribuudid:
  - Allkirjastamiseks kasutatav sertifikaat
  - Allkirjastamise aeg
  - Allkirjastamise asukoht
  - Allkirjastaja roll või resolutsioon
- Allkirjas sisaldub allkirjastaja sertifikaadi kehtivuse info
  - OCSP vastus
  - OCSP serveri sertifikaat

Antud mudeli tulemusena on võimalik allkirja kehtivust kontrollida ilma täiendava infota – allkirja kontrollija peab usaldama allkirjastaja sertifikaadi väljaandjat ja OCSP serveri sertifikaati.



DigiDoc konteineris sisalduvad algfailid (failid, mis allkirjastati). Allkirjad, mis on seotud allkirjastatud faili(de)-ga, kusjuures igas allkirjas sisaldub allkirjasta sertifikaat, kehtivuskinnitus ja kehtivuskinnituse teenuse sertifikaat.

DigiDoc süsteem kasutab ülaltoodud mudelile vastavate failide puhul "ddoc" laiendit.

.ddoc failide süntaks on kirjeldatud detailselt failiformaati kirjeldavas dokumendis [3] DigiDoc vorming.

4.1.2 BDOC vorming

Lisaks DigiDoc failivormingule toetab DigiDocService alates versioonist 3.5 ka BDOC 2.1 ajamärgendiga *(time-marking)* failivormingut. BDOC ajatempliga (*timestamp*) formaadi tugi on versioonis 3.8 vaid MobileCreateSignature meetodi kasutamisel, ülejäänud teenuse meetoditele lisandub ajatemplitega BDOC formaadi tugi teenuse versioonis 3.9. BDOC vormingu kirjelduse leiab spetsifikatsioonist [9].

Alates 2015. aastast on Eesti digitaalallkirja vaikimisi vorming BDOC, mistõttu on oluline infosüsteemidesse lisada BDOC failivormingu tugi. Lisainfo www.id.ee/bdoc

DigiDocService teenuse kasutajale mõeldud juhtnöörid BDOC failivormingule üleminekuks on leitavad aadressilt http://www.id.ee/index.php?id=37048.

4.2 Signeerimise algoritmid

DigiDocService toetab allkirjastamist nii RSA kui ka ECDSA (inglise keeles *Elliptic Curve Digital Signature Algorithm*) algoritmidega.

Teenus valib nii allkirjastamise kui autentimise korral algoritmi automaatselt. Rakenduse pakkuja saab kasutatud algoritmi tuvastada allkirjastaja sertifikaadi järgi (DigiDocService tagastab alati vastava sertifikaadi).

ECDSA on hetkel toetatud vaid Mobiil-ID puhul. Kui Mobiil-ID SIM-kaart ei ole ECDSA toega, kasutatakse RSA-algoritmi. Lisaks sõltub valik ka failivormingust: DDOC toetab ainult RSAd, kuid BDOC toetab nii RSAd kui ka ECDSAd.

Ühel allkirjastajal võib olla korraga olla mitu aktiivset sertifikaadipaari, kus iga paar on erineva algoritmi toega. Sellisel juhul valib DigiDocService sertifikaadi automaatselt.

Valiku loogika on järgmine:

- Kui Mobiil-ID omaniku SIM kaart on ECDSA toega, siis autentimisel (meetod MobileAuthenticate) kasutatakse alati ECDSA sertifikaate.
- Kui SIM kaart toetab nii ECDSA kui RSA algoritmi, siis BDOC failide allkirjastamisel (meetodid MobileSign ja MobileCreateSignature) kasutatakse ECDSA sertifikaate. Kuna DDOC failiformaat ei toeta ECDSA algoritmi, siis DDOC failide allkirjastamisel kasutatakse alati RSA algoritmi.

SIM kaartide puhul, millel on toetatud nii ECDSA kui RSA algoritmide kasutamine tagastab teenuse meetod GetMobileCertificate ECDSA alati sertifikaatide info ning ka meetod MobileSignHash kasutab sisemiselt alati ECDSA algoritmi.

RSAd kasutatakse 1024- ning 2048-bitiste võtmetega. ECDSA töötab NIST P-256 [8] kurvi peal ning allkirjad on kodeeritud vastavalt XMLDSig-spetsifikatsioonile [10] (lühidalt: kaks 256-bitist täisarvu üksteise järel; viimased on võrdse pikkuse saamiseks vasakult nullidega polsterdatud; tulemus kodeeritakse Base64 kujule). Kogu ECDSA allkiri on 512 biti pikkune.

5 Nõuded ja soovitused rakenduse pakkujale

5.1 Nõuded digitaalallkirjastamisele

- Tulenevalt „Digitaalallkirja seadusest“ peab digitaalallkiri koos selle kasutamise süsteemiga:
  1) võimaldama üheselt tuvastada isiku, kelle nimel allkiri on antud;
  2) võimaldama kindlaks teha allkirja andmise aja;
  3) siduma digitaalallkirja andmetega sellisel viisil, mis välistab võimaluse tuvastamatult muuta andmeid või nende tähendust pärast allkirja andmist.
- Kasutajad peavad olema PIN2 sisestamise eelselt informeeritud digitaalallkirjastamisega kaasnevatest õiguslikest tagajärgedest;
- Tuleb rakendada meetmeid selleks, et allkirjastatavad andmed oleksid allkirjastajale üheselt tõlgendatavad;
- Kasutajal peab olema võimalik veenduda allkirjastatavate andmete ja allkirjale lisatavate atribuutide (allkirjastamise asukoht, roll/resolutsioon) õigsuses juhul, kui neid kasutatakse;
- Tuleb tagada, et kasutajale allkirjastamise eelselt esitatud andmed vastavad tegelikult allkirjastatavatele andmetele;
- Kasutajale peab olema kättesaadav digitaalallkirjastamise järgselt tekkinud digitaalallkirjastatud fail. Nõue kehtib kõikidele toimingutele, mis kasutavad PIN2’e. Näiteks peale veebilehel maksekorralduse allkirjastamist peab allkirjastajal olema võimalik ligi pääseda allkirjastatud konteinerile. Antud nõue võimaldab allkirjastajal veenduda allkirjastatud dokumendi täpses sisus.

5.2 Nõuded Mobiil-ID toimingute käivitamiseks

Mobiil-ID toimingute käivitamine on võimalik kasutades DigiDocService meetodeid:

- MobileAuthenticate,
- MobileSign ja
- MobileCreateSignature.

Kõikide nende meetodite puhul on sisendparameetriteks Mobiil-ID kasutaja telefoninumber ja isikukood.

Kui soovite oma e-teenusesse lubada ka Leedu mobiilioperaatorite Mobiil-ID teenuse kasutajaid siis on mõlema sisendparameetri (isikukood ja telefoninumber) edastamine DigiDocService teenusele kohustuslik. Vastasel juhul Mobiil-ID toimingu algatamine ei õnnestu.

NB! Eesti mobiilioperaatorite puhul on soovitatav samuti edastada mõlemad sisendparameetrid. Nõue on plaanitud tulevikus muuta kohustuslikuks.

Ainult telefoninumbrit ei ole soovitatav kasutada ainukese identifikaatorina kuna telefoninumbrid on avalikud ning nii on võimalik läbi teie e-teenuse Mobiil-ID päringute saatmise algatamine kolmandatele isikutele.

Isikukoodi ja telefoninumbri mõlema kasutamise eelised on:

- Kasutaja eksimuse (sisestab näiteks telefoninumbri või isikukoodi mõne numbri valesti) tõttu on peaaegu välistatud, et päring saadetakse valele telefonile;
- Raskendatud on spämmimine, kuna isikukoodid ei ole avalikud;
- **Tulenevalt e-teenuse loogikast võib kasutajalt isikukoodi sisendparameetrina küsimise asemel kasutada ka muud väärtust, mille põhjal e-teenus teab kasutaja isikukoodi (näiteks kasutajatunnus, mis on infosüsteemis seotud isikukoodiga). Samuti võib e-teenus kasutaja telefoni numbrit meeles pidada ja seda ei pea kasutaja alati sisestama.**

Mobiil-ID toimingute käivitamisel on igal e-teenusel kohustuslik rakendada meetmeid (IP piirangud, spämmimist takistavad sisendparameetrid), mis teeksid võimatuks e-teenuse kaudu massilise Mobiil-ID autentimise või allkirjastamise päringute saatmise. Juhul, kui ühe teenuse kaudu tehakse üheaegselt tavapärasest määrast tunduvalt rohkem päringuid, on SK-l õigus, tagamaks teiste e-teenuste teenindamine ja/või lõpetamaks Mobiil-ID kasutajate vastu suunatud rünne, piirata päringute mahtu ületavale e-teenusele ligipääs.

Mobiil-ID toimingute käigus peab Mobiil-ID toimingut tegev e-teenus selgelt kuvama või edastama muul üheselt mõistetaval viisil kasutajale kontrollkoodi. Sealjuures tuleb silmas pidada, et kontrollkood peab olema nähtav ja loetav ka siis kui Mobiil-ID toimingut algatatakse mobiiltelefoni veebibrauseris. E-teenus peab kasutajale kuvama infoteksti, et enne telefoni Mobiil-ID PIN koodi sisestamist tuleb kontrollida rakenduses kuvatava kontrollkoodi kokkulangemist telefoni ekraanil kuvatavaga. Samuti tuleb kuvada hoiatust, et kui kontrollkoodid on erinevad tuleb toiming katkestada.

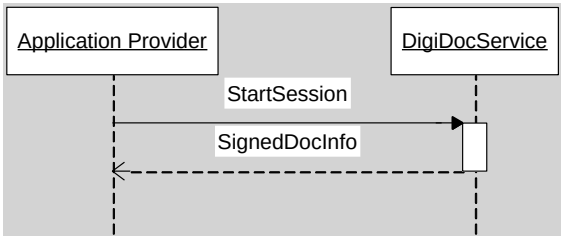
5.3 Tehnilised nõuded ja soovitused

- ID-kaardi ja Mobiil-ID-ga digitaalallkirjastamist ning autentimist võimaldavatest rakendustes soovitame tungivalt kasutada brauseri ja veebiserveri vahelises suhtluses krüpteeritud andmesidet (HTTPS ühendus).
- Mobiil-ID'ga autentimisel või allkirjastamisel tuleb rakendusel küsida teenusest regulaarselt toimingu olekuinfot (ehk *pollida* teenust), kaugel mobiiltelefoni kasutaja autentimise või allkirjastamisega jõudnud on. Juhul, kui mobiiliga allkirjastamist/autentimist tehakse veebirakendusest, on soovitatav veebilehel kasutada Ajax vahendeid, et olekuinfo järjekordsel küsimisel ei peaks lehte alati tervenisti uuesti laadima.
- DigiDocService teenusele saadetavate Digidoc konteineritele ja andmefailidele kehtib mahupiirang 4 MB. Punktis 8.1 on kirjeldatud, kuidas toimida suuremamahuliste failidega.

6 Peamised kasutusjuhud

6.1 Allkirjastatud faili verifitseerimine

Digitaalallkirjastatud dokumendi verifitseerimiseks kõige lihtsam moodus on kasutada StartSession päringut (kirjeldatud peatükis 8.1) väärtustades SigDocXML parameeter. Juhul, kui soovitakse saada ainult ülevaadet DigiDoc-i sisust ja edasisi allkirja lisamisi andmefailide/sertifikaatide lugemisi plaanis ei ole, on otstarbekas StartSession päring välja kutsuda bHoldSession parameetri väärtus oleks “false”. Sel juhul ei ole hilisemalt vajalik algatatud sessiooni sulgemine. StartSession päring tagastab allkirjastatud dokumendi info SignedDocInfo struktuurina, kust on välja loetavad allkirjastatud dokumendi olulisemad parameetrid.

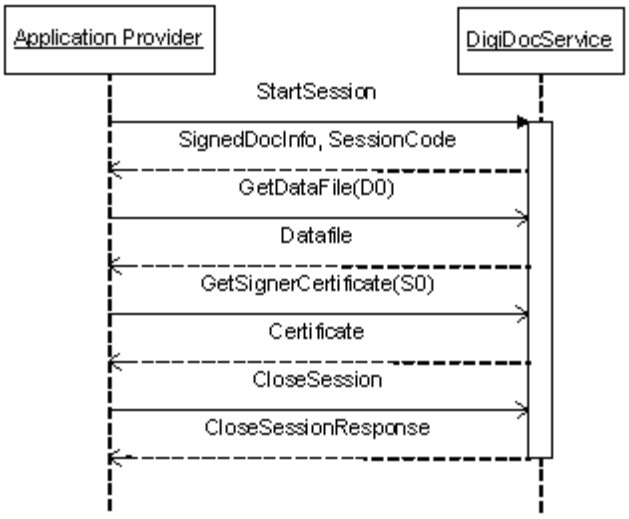


Kui StartSession kutsutakse välja bHoldSession parameetri väärtusega “true”, siis dokumendi verifitseerimise järgselt on võimalik pärida allkirjastatud dokumendi täiendavaid elemente:

- Andmefaili infot – GetDataFile meetod;
- Allkirjastaja sertifikaati – GetSignerCertificate meetod;
- Allkirja kehtivuskinnitust – GetNotary meetod;
- Kehtivuskinnituse sertifikaati – GetNotaryCertificate meetod.

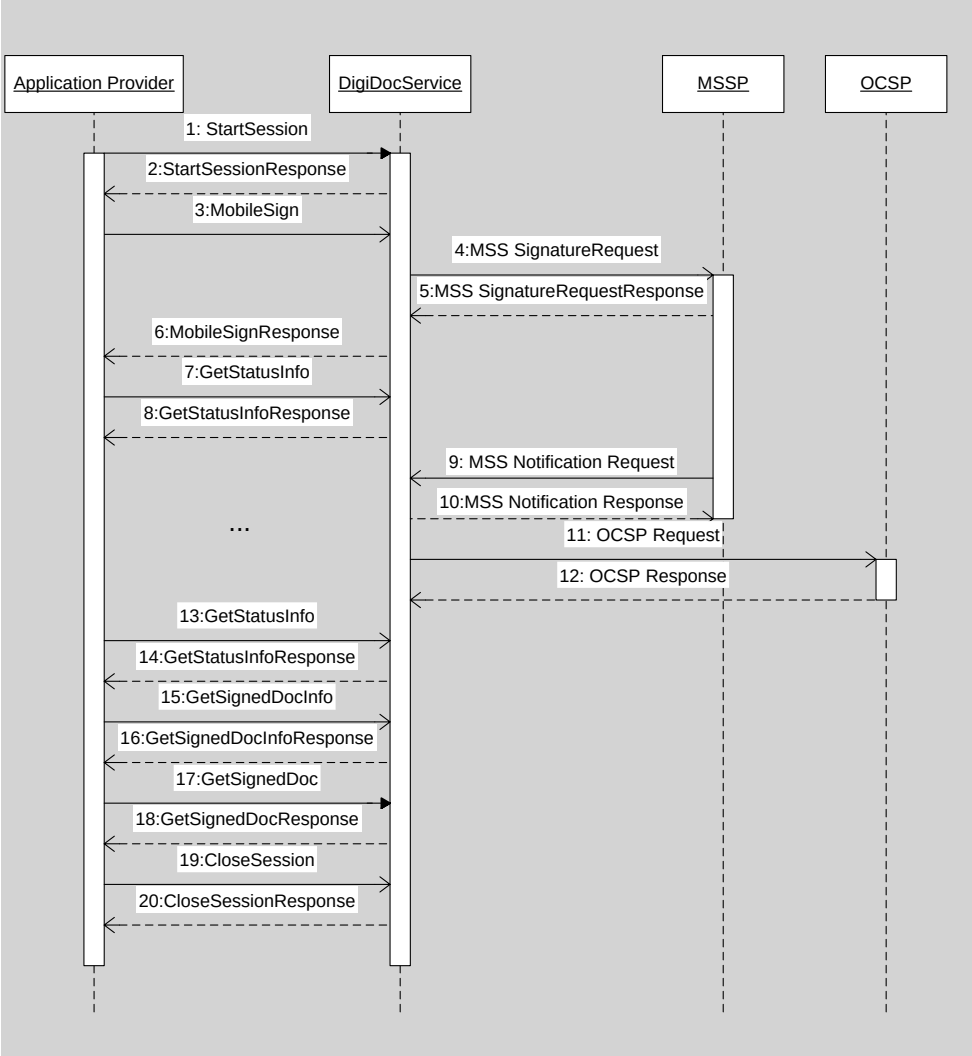
StartSessioni kasutamisel bHoldSession=true korral on vajalik hiljem sessioon CloseSession meetodiga sulgeda.

Näidis kasutusjuhu jadadiagramm:



6.2 Allkirjastamine

6.2.1 Mobiiliga Allkirjastamine asünkroonselt Client-Server režiimis



1. Teenust kasutav rakendus saadab StartSession päringu käigus allkirjastamist vajavad failid (DigiDoc faili või algfailid).
2. StartSession päringu tulemusena tagastatakse muuhulgas loodud sessiooni identifikaator, mida tuleb kasutada järgnevates päringus.
3. Allkirjastamise käivitamiseks saadab rakendus MobileSign päringu. Kui soovitakse allkirjastada korraga mitut algfaili on võimalik enne MobileSign päringu saatmist AddDataFile päringuga lisada täiendavaid andmefaile.
4. DigiDocService edastab signeerimispäringu MSSP teenusele, kes omakorda edastab selle telefonioperaatori kaudu kasutaja telefonile.
5. MSSP tagastab kas veakoodi või info päringu täitmise kohta.
6. DigiDocService tagastab teenust kasutavale rakendusele MobileSign päringu vastuse, milleks on kas veakood või info signeerimispäringu õnnestumise kohta.

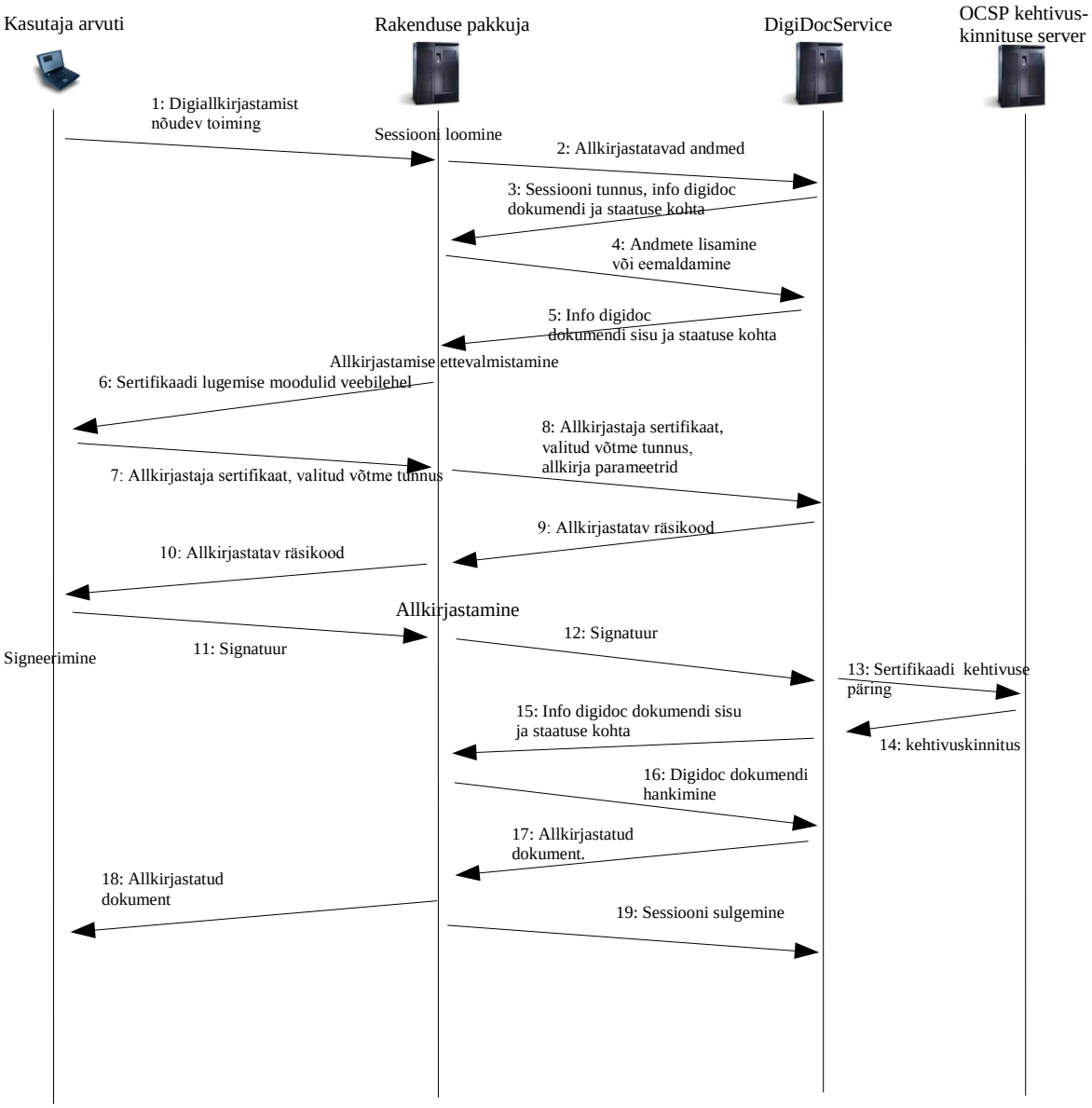
7, 8. Järgnevalt peab asünkroonse client-server režiimi korral rakendus saatma regulaarselt mingi väikese intervalli (näiteks mõne sekundi) järel

DigiDocService'le GetStatusInfo päringu kuni signeerimise toiming on kas õnnestunud või ebaõnnestunud.

9. MSSP teenus saadab signeerimise õnnestumise/ebaõnnestumise kohta teate. Kui signeerimine õnnestub, saadetakse DigiDocServicele ka signatuur.
10. DigiDocService tagastab MSSP-le info signatuuri kättesaamise kohta
11. Saanud kätte signatuuri, teeb DigiDocService OCSP kehtivuskinnituse teenusesse päringu allkirjastaja sertifikaadi kehtivuse kohta.
12. Kehtivuskinnituse teenus tagastab kehtivuskinnituse. Sessioonis olevale DigiDoc failile lisatakse allkiri, mis sisaldab muuhulgas signatuuri ja kehtivuskinnitust.
13. Teenusele tehakse järjekordne GetStatusInfo päring
14. Seekord tagastab GetStatusInfo vastuse signeerimistoimingu õnnestumise või ebaõnnestumise kohta
15. Teenust kasutava rakenduse poolt tehakse GetSignedDocInfo päring dokumendi staatuse kohta.
16. DigiDocService tagastab info dokumendi staatuse, sealhulgas allkirja lisamise õnnestumise koha.
17. Rakendus küsib GetSignedDoc meetodiga allkirjastatud DigiDoc faili sisu.
18. DigiDocService tagastab DigiDoc fail. Juhul, kui StartSession päringu käigus ei edastatud teenusele andmefailide sisu, tuleb teenust kasutaval rakendusel ise DigiDoc konteinerisse lisada andmefailide sisu.
19. Rakendus sulgeb CloseSession päringuga sessiooni.
20. Teenus kustutab sessioonis oleva info ja tagastab vastuse sessiooni eduka sulgemise kohta.

6.2.2 Kiipkaardiga allkirjastamine

Käesolev näide on toodud digitaalallkirjastamist võimaldava veebilehe näitel.



1. Digitaalallkirjastamist pakkuva rakenduse kasutaja on valinud mingi toimingu, mis eeldab andmete allkirjastamist. Kasutaja alustab allkirjastamise protsessi, klõpsates rakenduse pakkuja veebiteenuses vastavat nuppu või linki.

2. Allkirjastamiseks valitud andmed saadetakse StartSession päringuga DigiDocService-le - sellega algatatakse uus sessioon. Iga sessioon on seotud ühe (allkirjastatud) dokumendiga. Ühes allkirjastatud dokumendis

võib aga olla mitu andmekogumit (algfaili). Rakendus saadab teenusele kas:

a. allkirjastatava faili;
b. allkirjastatava faili metainfo ja räsi (faili sisu on eemaldatud);
c. puhul kogu allkirjastatava konteineri või
d. puhul allkirjastatava konteineri, millest on eemaldatud andmefailide keha(d) (eemaldatud on DataFile märgiste vahele jääv faili sisu).

Allkirjastamiseks vajalike andmete saatmise viisid on täpsemalt kirjeldatud peatükis 8.1. StartSession päringu käigus vastuvõetud andmed talletatakse sessioonis.

3. Rakendusele tagastatakse SessionCode, mis võimaldab sessioonis olevate andmetega järgmisi toiminguid teostada.
4. 4,5 Enne allkirjastamist võib rakendus lisada täiendavaid andmefaile (AddDataFile päring või eemaldada mõne andmefaili (RemoveDataFile päring) või teostada sessioonis olevate andmetega muid toiminguid.
5. Toimingute järgselt tagastatakse hetkel sessioonis oleva dokumendi info.
6. Allkirjastamismoodul on integreeritud allkirjastamist pakkuvale veebilehele. Lehel olev allkirjastamise komponent loeb allkirjastaja kiipkaardilt sertifikaadi info. Allkirjastamismooduli laadimiseks soovitame kasutada Javascripti klienditeeki idCard.js, mille kohta leiate info http://www.id.ee-st.
7. Allkirjastaja kiipkaardilt on välja loetud sertifikaat edastatakse koos muude kasutaja poolt sisestatud allkirja atribuutidega allkirjastamise funktsionaalsust pakkuvasse veebiserverisse.
8. Allkirja parameetrid edastatakse DigiDocServicele kasutades PrepareSignature päringut.
9. DigiDocService lisab sessioonis olevale dokumendile uue allkirja info – allkirjasta sertifikaadi ja allkirja parameetrid ning arvutab välja räsi, mille allkirjastaja peab signeerima ja saadab selle rakenduse pakkujale PrepareSignature vastuses.
10. Allkirjastatav räsi kuvatakse koos allkirjastamise mooduliga kasutajale. Kasutaja vajutab lehel olevat allkirjastamise nuppu, mispeale allkirjastamismoodul toimetab ära signeerimise operatsiooni, sh küsib PINi. Moodustatud signatuur pannakse vormi peidetud väljale ja saadetakse allkirjastamisfunktsionaalsust pakkuvale veebilehele.
11. Signatuur edastatakse signeerimist pakkuvale veebiserverile (rakenduse pakkujale).
12. Signatuur edastatakse DigiDocServicele FinalizeSignature päringuga.
13. DigiDocService kontrollib allkirjastaja sertifikaadi kehtivust OCSP kehtivuskinnituse teenusest.
14. OCSP kehtivuskinnituse server tagastab allkirja kehtivuskinnituse.
15. Kui kinnitus oli positiivne, st allkirjastaja sertifikaat kehtis, lisab DigiDocService kogu info (allkirjastaja signatuuri ja kehtivuskinnituse) moodustatavale allkirjale. Nüüd on sessioonis olev DigiDocile lisatud allkiri terviklik. DigiDocService tagastab SignedDocInfo digitaalallkirjastamist pakkuvale rakendusele.
16. Rakendus pärib GetSignedDoc päringuga DigiDoc faili sisu.
17. DigiDocService tagastab sessioonis oleva DigiDoc dokumendi, milles sisaldub ka lisatud allkiri.
18. Kasutajat informeeritakse, et allkirjastamine on edukalt lõpetatud ja kasutaja saab allkirjastatud DigiDoc faili alla laadida oma arvutisse. NB!

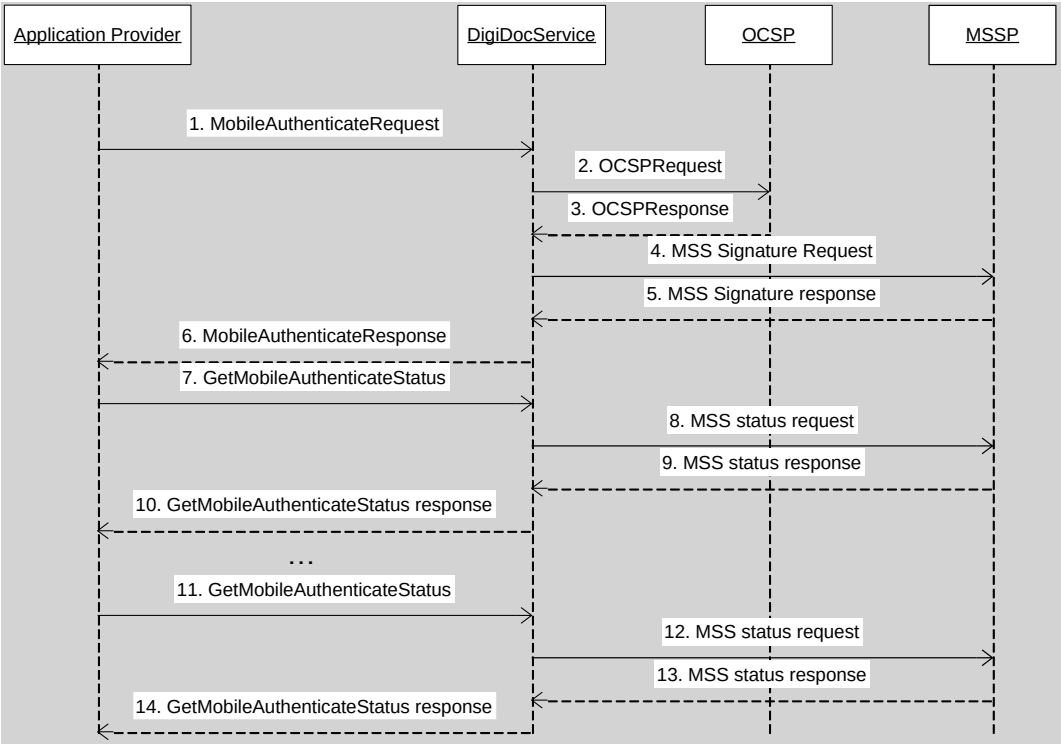
Juhul kui StartSession ja AddDataFile päringutes ei saadetud serverisse andmefailide sisu (variandid b ja d) on vajalik teenusest saadud DigiDoc faili andmefailide kehade lisamine. <DataFile> märgisest tuleb muuta ära ContentType, eemaldada viide räsikoodile ja lisada <DataFile> märgiste vahele andmefailide sisud Base64 kujul. Võimaluse korral kontrollitakse täiendavalt allkirjade kehtivust ja faili terviklikkust.

19. Viimase sammuna on digitaalallkirjastamist pakkuv rakendus viisakas ja sulgeb CloseSession päringuga sessiooni, mispeale teenus kustutab sessiooni käigus talletatud andmed.

6.3 Autentimine

6.3.1 Mobiil-ID autentimine asünkroonselt klient-server režiimis

Kasutusjuht kirjeldab Mobiil-ID'ga kasutaja autentimist.



1. Rakendus saadab DigiDocServicele MobileAuthenticate päringu käigus autentimiseks vajalikud andmed (kasutaja info, autentimisel kasutajale kuvatav tekst, keel)
2. Teenus saadab OCSP kehtivuskinnituse teenusele kasutaja autentimiseks sertifikaadi kehtivuse päringu.
3. OCSP kehtivuskinnituse teenus tagastab info autentija sertifikaadi kehtivuse kohta. Kui sertifikaat kehtib, suundutakse sammu 4 juurde, vastasel juhul sammu 6 juurde.
4. DigiDocService saadab MSSP teenuse kaudu kasutaja telefonile autentimispäringu.

5. MSSP tagastab kas veakoodi või info autentimispäringu saatmise õnnestumise kohta.
6. Sõltuvalt sellest, kas autentija sertifikaat kehtis ja autentimispäringu edastamine õnnestus, tagastatakse rakenduse pakkujale positiivne või negatiivne vastus; positiivses vastuses sisaldub ka info autenditava isiku kohta.
7. Sõltuvalt kasutatavast režiimist hakkab rakenduse pakkuja küsima perioodiliselt allkirjastamistoimingu staatust või ootab staatusinfo automaatset saatmist DigiDocService poolt. Antud näide käsitleb teenuse kasutamist klient-server režiimis, mistõttu rakenduse pakkuja peab perioodiliselt saatma DigiDocServicele autentimistoimingu staatuse küsimise päringu: *GetMobileAuthenticateStatus*.
8. DigiDocService pärib omakorda MSSP teenuselt autentimisetoimingu staatust.
9. MSSP teenus vastab autentimispäringu staatuse kohta.
10. Info autentimistoimingu staatuse kohta saadetakse edasi rakenduse pakkujale.
11. 12. 13. 14 jne sammudes korratakse 7, 8, 9, 10 sammudes tehtud toimingut niikaua, kuni saabub veainfo või positiivne vastus autentimistoimingu õnnestumise kohta.

6.3.2 Kiipkaardiga autentimine

ID-kaardiga autentimise ühe osana - autentimissertifikaadi kehtivusinfo küsimiseks - saab kasutada teenuse meetodit CheckCertificate.

7 Autentimisega seotud teenuse päringud ja vastused

Kõik päringud ja vastused on RPC-encoded kujul, kasutatakse UTF-8 kodeeringut.

7.1 MobileAuthenticate

Meetod Mobiil-ID autentimise protsessi käivitamiseks.

Meetodi täitmisel kontrollitakse esmalt tuvastatava isiku Mobiil-ID digitaalset isikutuvastamist võimaldava sertifikaadi kehtivust. Sertifikaadi kehtivuse korral edastatakse autentija telefonile autentimispäring, vastasel korral tagastatakse viga. Päringu tulemusena tagastatakse rakendusele autenditava kasutaja info, autentijale kuvatav kontrollkood ning rakenduse pakkuja soovi korral ka isikutuvastusesertifikaat ja selle kehtivusinfo.
Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Autenditava isiku isikukood. Kohustuslik on kas IDCode või PhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud IDCode ja PhoneNo
CountryCode	String(2)	-	Isikukoodi välja andnud riik, kasutatakse ISO 3166

			2 tähelisi riigikoode (näiteks: EE).
PhoneNo	String	+	Autenditava isiku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301. Kohustuslik on kas IDCode või PhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud IDCode ja PhoneNo (vt. peatükk 5.2). Kui element “PhoneNo” on määratud, siis teenuse siseselt lähtutakse prefiksis määratud riigi tunnusest (sõltumata elemendi "CountryCode" väärtusest)
Language	String(3)	+	Telefonile kuvatavate teadete keel. Kasutatakse: 3-tähelisi koode suurtähtedes. Võimalikud variandid: (EST,ENG,RUS,LIT).
ServiceName	String(20)	+	Autentimisel telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki. Eelnevalt on vajalik kasutatava teenuse nimetuse kokkuleppimine teenuse pakkujaga.
MessageToDisplay	String(40 baiti)	-	Täiendav tekst, mis autentimise PIN-i küsimise eelselt lisaks teenuse nimetuse kasutaja telefonile kuvatakse. Maksimaalne pikkus 40 baiti (ladina tähtede puhul tähendab see ühtlasi ka 40 sümboli pikkust teksti, aga näiteks kirillitsa teksti puhul võidakse tähti kodeerida 2 baidistena ja siis ei saa saata pikemat kui 20-sümbolilist teksti).
SPChallenge	String(20)	-	Rakenduse pakkuja poolt genereeritud juhuslik 10 baidine tekst, mis on osa (autentimise käigus) kasutaja poolt signeeritavast sõnumist. Edastatakse HEX stringina. **NB!** Suurema turvalisuse huvides on soovitatav see väli alati täita, iga kord erineva juhusliku väärtusega. Kui autentimine õnnestub, on soovitatav ka kontrollida, et kasutaja poolt allkirjastatud väärtus tõepoolest ka sisaldab antud SPChallenge-i väärtust. Täpsem info viimase verifitseerimise kohta on peatükis „GetMobileAuthenticateStatus“, „Signature“-elemendi kirjelduse all.
MessagingMode	String	+	Autentimise toimingu vastuse tagastamise viis. Võimalikud variandid: - “asynchClientServer” – rakendus teeb pärast MobileAuthenticate meetodi väljakutsumist täiendavaid staatuspäringuid (kasutades meetodit *GetMobileAuthenticateStatus*). - “asynchServerServer” – toimingu lõppemisel või vea tekkimisel saadetakse vastus kliendirakendusele asünkroonselt (vt. parameeter AsyncConfiguration).
AsyncConfiguration	Integer	-	Määrab asünkroonselt vastuse tagasisaatmise

			konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul kui MessagingMode on “asynchServerServer”. Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel. Hetkel on toetatud vastuse tagasi saatmine kasutades Java Message Services (JMS) liidest.
ReturnCertData	Boolean	-	Kui väärtus on “TRUE”, tagastatakse vastuses autenditava isiku sertifikaat. Sertifikaat on vajalik, kui rakenduse pakkuja soovib talletada ja iseseisvalt kontrollida signatuuri korrektsust ja kehtivusinfot.
ReturnRevocationData	Boolean	-	Väärtuse “TRUE” korral tagastatakse sertifikaadi kehtivusinfo vastuses RevocationData väljal.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	loodud sessiooni identifikaator
Status	String	Toimingu edukal täitmisel “OK” **NB!** Antud toimingule “OK” vastuse saamine ei tähenda, et kasutaja on tuvastatud – kasutaja autentimiseks tuleb teha täiendavad staatusepäringud kuni autentimistoimingu olek on “USER_AUTHENTICATED”. Juhul, kui meetodi väljakutsel juhtub viga, tagastatakse SOAP veaobjekt. SOAP veaobjektide kirjeldus ja veakoodid on toodud peatükis 9.4.
UserIDCode	String	Autenditava isiku isikukood. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime “Serial Number” väljalt.
UserGivenname	String	Autenditava isiku eesnimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime G (Given name) väljalt.
UserSurname	String	Autenditava isiku perekonnanimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime SN (Surname) väljalt.
UserCountry	String(2)	Autenditava isiku riik, kasutatakse ISO 3166 2 tähelisi riigikoode. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime C (Country) väljalt.
UserCN	String	Autenditava isiku isikutuvastuse sertifikaadi põhinimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime CN (Common Name) väljalt.
CertificateData	String	Autenditava isiku isikutuvastuse sertifikaat Base64 kujul (tagastatakse ainult juhul, kui päringus ReturnCertData väärtus on “TRUE”, vastasel korral tagastatakse tühi string.
ChallengeID	String	4 tähemärgiline kontrollkood, mis arvutatakse kasutaja telefonile signeerimiseks saadetava Challenge väärtuse põhjal. Antud kontrollkood tuleb mobiilautentimist võimaldaval rakendusel kuvada kasutajale ja selle kaudu on võimalik kasutajal veenduda päringu autentsuses.

		NB! Mobiil-ID autentimise rakendus peab paluma kasutajal kontrollida rakenduses ja telefonil kuvatava kontrollkoodi kokkulangevust.
Challenge	String	Kasutaja poolt autentimisel allkirjastatav sõnum, koosneb rakenduse looja poolt saadetud sõnumist (SPChallange, 10 baiti) ja teenuse poolt lisatust (samuti 10 baiti). Tagastatakse vaid juhul, kui päringus SPChallenge väli on väärtustatud.
RevocationData	String	Sertifikaadi kehtivusinfo (OCSP kehtivuskinnituse teenuse vastus) Base64 kujul. Tagastatakse ainult juhul, kui päringus ReturnRevocationData parameetri väärtus on “TRUE”, vastasel korral tagastatakse tühi string.

Kui kasutatakse AsynchClientServer režiimi, tuleb pärast vastuse saamist hakata teenusele saatma GetMobileAuthenticateStatus päringuid veendumaks, et kasutaja sisestab isikutuvastuse PIN-i ja saab tuvastatud.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 15 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda. Mobiil-ID toimingud aeguvad hiljemalt 4 minuti jooksul.

Juhul, kui kasutatakse “asynchServerServer” režiimi saadetakse autentimise toimingu lõppemisel automaatselt teenuse kasutajale vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	**Tüüp**	**Kirjeldus**
Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel “USER_AUTHENTICATED”. Teised võimalikud olekud on kirjeldatud GetMobileAuthenticateStatus päringu vastuses.
Data	String	Autentimise käigus moodustatud signatuur PKCS#1 konteinerina Base64 kujul. Tagastatakse ainult juhul, kui teenuse kasutaja on ette andnud SPChallange, vastasel juhul on väärtus tühi. Signatuuri esituskuju on täpsemalt kirjeldatud peatükkides 7.2 (vastuse parameetri Signature kirjelduses) ja peatükis 4.2.

7.2 GetMobileAuthenticateStatus

Antud meetodit kasutatakse sünkroonses režiimis Mobiil-ID autentimise toimingu staatuse pärimiseks.

Päring:

Parameeter	**Tüüp**	**K**	**Kirjeldus**
Sesscode	Integer	+	Sessiooni identifikaator (kasutada väärtust, mis

			tagastati MobileAuthenticate vastuses).
WaitSignature	Boolean	+	Kui TRUE, siis päringule enne vastust ei tagastata, kui telefonilt on signatuuri väärtus saabunud, või on juhtunud viga. FALSE korral tagastatakse kohe vastus ja rakendus peab GetMobileAuthenticate meetodi väikese viite (2-10 sekundit) järel uuesti välja kutsuma.

Vastus:

Parameeter	Tüüp	Kirjeldus
Status	String	Mobiilautentimise protsessi olek: - OUTSTANDING_TRANSACTION– autentimine alles toimub; - USER_AUTHENTICATED – isik autenditud; - NOT_VALID – toiming on lõppenud, kuid kasutaja poolt tekitatud signatuur ei ole kehtiv. - EXPIRED_TRANSACTION – tegevus on aegunud; - USER_CANCEL – kasutaja katkestas; - MID_NOT_READY - Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti - PHONE_ABSENT – telefon ei ole levis; - SENDING_ERROR – Muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - INTERNAL_ERROR – teenuse tehniline viga
Signature	String	Autentimise käigus moodustatud signatuur Base64 kujul. Tagastatakse ainult juhul, kui MobileAuthenticate päringus oli määratud SPChallange, vastasel juhul on väärtus tühi. **NB!** Kuigi kontroll tehakse ka DigiDocService'i sees, siis suurema turvalisuse huvides on rakenduse loojal võimalik signatuuri veel täiendavalt verifitseerida, kasutades selleks allkirjastatavat sõnumit (väli Challenge MobileAuthenticate meetodi vastusest, millest 10 esimest baiti peab olema DigiDocService'it kasutava rakenduse poolt ette antud SPChallange), avalikku võtit kasutaja autentimissertifikaadist ning arvutatud signatuuri. Sõltuvalt kasutatava sertifikaadi tüübist on signatuur arvutatud, kas RSA või ECDSA algoritmi järgi. Autentimisallkirjad on tehtud *ilma* räsifunktsioonideta (nii RSA kui ka ECDSA korral). Näiteks kui „Challenge"- välja väärtus oli "123456789012345678903693330D3483DAED0496D" (millest esimene pool oli valitud rakenduse pakkuja poolt), siis allkirjastamine toimib viisil, nagu antud väärtus oleks juba räsifunktsiooni väljund. Seetõttu RSA

		puhul pannakse allkirjastatava väärtuse ette ka tavapärane SHA-1 prefiks (kuigi väärtus tegelikult ei tulnud SHA-1 räsifunktsioonist). ECDSA korral tavapäraselt prefikseid ei kasutata. Signatuuri esituskuju on kirjeldatud käesoleva dokumentatsiooni peatükis 4.2.

Kui vastuses on Status väärtus ei ole OUTSTANDING_TRANSACTION, siis meetodi välja kutsumise järgselt sessioon suletakse.

7.3 CheckCertificate

Antud meetodit saab kasutada sertifikaatide (muuhulgas ID-kaardi ja Digitempli või muu kiipkaardi sertifikaatide) kehtivusinfo kontrollimiseks – mugavamaks täienduseks senisele võimalusele küsida sertifikaatide kehtivusinfot kehtivuskinnitusteenuse (OCSP) käest. Lisaks tagastab meetod (olulisemate) sertifikaadiväljade väärtused.

Lisaks tagastab meetod kehtivusinfot Sertifitseerimiskeskuse kehtivuskinnitusteenuse poolt teenindatavate välismaiste sertifitseerijate sertifikaatide kohta. Teenindatavate välismaiste sertifitseerijate infot saamiseks tuleb pöörduda SK poole.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Certificate	String	+	Kontrollitava sertifikaadi andmed BASE 64 kujul. Sertifikaadi andmed võivad sisaldada ka sertifikaadi PEM formaadile omaseid „---BEGIN CERTIFICATE---„ ja „---END CERTIFICATE---„ ridu
ReturnRevocationData	Boolean	-	Väärtuse TRUE korral tagastatakse sertifikaadi kehtivusinfo vastuses RevocationData väljal.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	loodud sessiooni identifikaator
Status	String	Sertifikaadi kehtivusinfo. - GOOD – sertifikaat kehtib - REVOKED – sertifikaat on tühistatud - UNKNOWN – sertifikaati ei ole kunagi välja antud või on tegu tundmatu sertifitseerijaga - EXPIRED – sertifikaat on aegunud (lõpu kuupäev on vanem kui hetkekuupäev) - SUSPENDED – sertifikaat on peatatud
UserIDCode	String	Sertifikaadiomaniku isikukood. SK poolt välja antud sertifikaatide korral võetakse väärtus sertifikaadi eraldusnime “Serial Number” väljalt.

UserGivenname	String	Sertifikaadiomaniku eesnimi. Väärtus võetakse sertifikaadi eraldusnime G (Given name) väljalt.
UserSurname	String	Sertifikaadiomaniku perekonnanimi. Väärtus võetakse sertifikaadi eraldusnime S (Surname) väljalt.
UserCountry	String(2)	Sertifikaadiomaniku riik, kasutatakse ISO 3166 2-tähelisi riigikoode. Väärtus võetakse sertifikaadi eraldusnime C (Country) väljalt.
UserOrganisation	String	Sertifikaadiomaniku organisatsioon, väärtus võetakse sertifikaadi eraldusnime O (Organisation) väljalt.
UserCN	String	Sertifikaadi põhinimi. Väärtus võetakse sertifikaadi eraldusnime CN (Common Name) väljalt.
Issuer	String	Sertifikaadi väljaandja (Issueri) eraldusnimi (CN).
KeyUsage	String	Sertifikaadiga seotud (salajase) võtme kasutusalad
EnhancedKeyUsage	String	Võtme laiendatud kasutusalad
RevocationData	String	Sertifikaadi kehtivusinfo (OCSP kehtivuskinnituse teenuse vastus) Base64 kujul. Tagastatakse ainult juhul, kui päringus ReturnRevocationData parameetri väärtus on TRUE, vastasel korral tagastatakse tühi string.

Tagastatavad väärtused on UTF8 kodeeringus.

8 Digitaalallkirjastamisega seotud teenuse meetodid

8.1 StartSession

Enamasti alustatakse transaktsiooni veebiteenusega kasutades StartSession meetodit. Päringuga võib saata teenusele ka andmefaile, millega hiljem opereerida. StartSessioni kasutamiseks on 3 erinevat võimalust:

1) Päringu käigus saadetakse teenusele juba valmis DigiDoc või BDOC fail, millele soovitakse lisada allkirja, kontrollida faili sisu või eraldada andmefaili sisu. Sellisel juhul täidetakse „SigDocXML“-parameeter, kuid „datafile“-parameeter jäetakse tühjaks.
2) Teenusele saadetakse andmefail, mille põhjal soovitakse moodustada uut DigiDoc-faili (BDOC pole selle mooduse juures toetatud – BDOCi jaoks vt meetodit CreateSignedDoc). Sellel juhul jäetakse „SigDocXML“-parameeter tühjaks, kuid täidetakse „datafile“-parameeter.
3) Luuakse tühi, (hetkel veel) ilma andmefailita sessioon. Viimane on kasulik näiteks meetodi CreateSignedDoc väljakutsumiseks, millega saab luua uusi BDOC-konteinereid. Antud juhul jäetakse tühjaks nii parameeter „SigDocXML“ kui ka „datafile“.

StartSession päringu käigus tagastatakse unikaalne sessiooni identifikaator, mis tuleb lisada kõigile antud transaktsiooni käigus teostatud toimingutele.

Päring:

Parameeter	Tüüp	K	Kirjeldus

SigningProfile	String	-	Parameetrit ignoreeritakse antud operatsiooni juures. Väärtus võib olla ka tühi
SigDocXML	String	-	BDOC või DigiDoc dokument. DigiDoc dokument on XML kujul, mis on viidud HTML escaped kujule. Näiteks “<DataFile>” peab olema viidud kujule „<DataFile>“. BDOC formaadis konteiner tuleb teenusele saatmiseks eelnevalt BASE64-kodeerida.
bHoldSession	Boolean	-	lipp, mis määrab kas StartSession päringu käigus saadetud andmeid hoida sessioonis või kustutada teenusele saadetud info kohe pärast vastuse tagastamist
datafile	Datafile	-	antud element võimaldab StartSession päringu käigus saata teenusele andmefail, mille põhjal moodustatakse DigiDoc konteiner (BDOC-formaat pole antud kasutusjuhu puhul toetatud – uue BDOCi loomiseks vt käsku CreateSignedDoc). Näiteks cv.pdf saatmisel tekitatakse cv.ddoc mis sisaldab esialgu ainsa andmefailina cv.pdf-i. Datafile struktuur on kirjeldatud käesolevas dokumendis peatükis 9.3. Andmefaili lisamisel ei ole vajalik määrata faili identifikaatorit. Vaikimisi tekitatakse DIGIDOC-XML 1.3 fail.

NB! Teenusele ei tohi saata korraga SigDocXML kui ka Datafile andmeid, kuna nad on üksteist välistavad.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	Väärtus „OK“ või veastring.
Sesscode	Integer	Sessiooni kood, mida kasutatakse antud transaktsiooni edasistes päringutes.
SignedDocInfo	SignedDocInfo	Juhul, kui StartSession päring sisaldas andmefaili või DigiDoc faili, tagastatakse vastuses SignedDocInfo struktuur käesoleva dokumendi peatükis 9.1 esitatud kujul

8.1.1 HASHCODE kuju

DigiDocService teenusele saadetavatele allkirjastatud konteineritele ja andmefailidele kehtib mahupiirang 4 MB. Suuremate failide üle võrgu DigiDocService-isse saatmine võib võtta palju aega, seetõttu töökiiruse huvides on soovitatav teenusesse mitte saata tervet andmefaili, vaid saata ainult andmefaili info ning andmefaili räsi – ja seda mõlemal juhul: andmefailide saatmise korral (kui kasutatakse StartSession’i Datafile parameetrit) ning ka teenusele DigiDoc/BDOC konteineri saatmisel, kui kasutatakse StartSession’i SigDocXML parameetrit. Allpool on mõlema juhu kohta selgitavad näited.

HASHCODE kuju kasutamiseks tuleb DigiDoc või BDOC-konteiner teisendada enne teenusele saatmist HASHCODE-kujule, milles failide sisud on asendatud nende räsidega. Analoogselt tuleb teenuselt tagasi tulnud konteiner teisendada tagasi tavakujule, mida saab seejärel taas verifitseerida ka standardvahenditega (näiteks DigiDoc3 klient tarkvaraga). Täpne HASHCODE-konteineri kuju sõltub kasutatavast vormingust (BDOC või DDOC).

8.1.1.1 BDOC vorming ja HASHCODE

8.1.1.1.1 BDOC konteineri HASCODE kujule teisendamine

BDOC vormingu korral tuleb (enne päringu sooritamist) viia konteiner HASHCODE kujule järgmiselt:

1) Eemaldada konteinerist **kõik allkirjastatavad** failid. Kuna BDOC kujutab endast ZIP-formaadis pakitud faili, saab seda operatsiooni sooritada standardsete ZIP-teekidega (allkirjastatavad failid asuvad ZIP-faili juurkataloogis).
2) Lisada konteinerisse eemaldatud failide räsid. Selleks tuleb BDOC konteinerisse (mis on alati ZIP-formaadis) lisada 2 räsifaili:

   - `META-INF/hashcodes-sha256.xml`
   - `META-INF/hashcodes-sha512.xml`

   Esimene räsifail sisaldab allkirjastatavate failide SHA-256 räsisid, teine SHA-512 räsisid. Mõlema faili formaat on sama: kõikide allkirjastavate failide kohta on kirjas nende täispikad failinimed, räsid Base64-kodeeritult (olenevalt failist kas SHA-256 või SHA-512), ning failide pikkused baitides. (Täpne XML-skeem on toodud allpool). Räsid arvutatakse otse vastavate failide sisu pealt (st et mitte üle XML-elementide, erinevalt DDOC-formaadist).

   Näiteks kui konteiner sisaldab 2 dokumenti nimedega file1.txt ning File2.docx (näidisfailid on alla laetavad http://www.id.ee/public/bdoc_hashcode_example.zip), on vastavad räsifailid järgmised:

   - *META-INF/hashcodes-sha256.xml*:

```
<?xml version="1.0" encoding="utf-8"?>
<hashcodes>
    <file-entry full-path="file1.txt"
hash="fo+6a5j64VcKWJwvXsJE8PlB3tAdQ8/uwHAL5AEWmbk=" size="189"/>
    <file-entry full-path="File2.docx"
hash="3v5ZupBhiNxkCmmVKbtwwJKVCKxTZrQDPpNKF02ZiPo=" size="11665"/>
</hashcodes>
```

   - *META-INF/hashcodes-sha512.xml*:

```
<?xml version="1.0" encoding="utf-8"?>
<hashcodes>
    <file-entry full-path="file1.txt"
hash="WIJZPgHWMrqfHqH7Arfjo8ymMZvI0IUgG8G8UESbnHXcpEPgOKutPph1GYOcSprj08VZ
a0m+myhlVPH29ThjIA==" size="189"/>
    <file-entry full-path="File2.docx"
hash="3z7gxofgCPoX2feWB9TQhUIvOlhsxm9RVR3iEFcCZ7uPcZuRc+KS9evmBC6bAMUnQOvk
```

```
    ygXNTPfTIKb50krYYg==" size="11665"/>
    </hashcodes>
```

Räsifailid peavad vastama järgmisele XML-skeemile:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="hashcodes" type="hashcodesType"/>

  <xs:complexType name="fileEntryType">
    <xs:attribute name="full-path" type="xs:string" use="required"/>
    <xs:attribute name="hash" type="xs:string" use="required"/>
    <xs:attribute name="size" type="xs:long" use="required"/>
  </xs:complexType>

  <xs:complexType name="hashcodesType">
    <xs:sequence>
      <xs:element name="file-entry" type="fileEntryType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

NB! Kuigi ZIP-faili teisendusi võib sooritada standardsete ZIP-faili töövahenditega, tuleb siiski jälgida, et ei rikutaks faili sisemist struktuuri. ASiC-standard esitab „mimetype“-failile järgmised nõuded:

- „mimetype“ fail peab jääma esimeseks failiks ZIP-arhiivis
- „mimetype“ fail ei tohi olla pakitud kujul (st et tuleb kasutada nullpakkimist; näiteks võib pakkimismeetod olla olla „*stored*“, aga mitte „*deflated*“).

Peale antud teisendusi on konteinerfaili sisu analoogne järgmise pildiga - lühidalt korrates: lisandunud on räsifailid ning andmefailid on eemaldatud:

```
├── META-INF
│   ├── hashcodes-sha256.xml
│   ├── hashcodes-sha512.xml
│   ├── manifest.xml
│   └── signatures0.xml
└── mimetype
```

Näidisfailid ja neile vastavad BDOC konteinerid on alla laetav aadressilt http://www.id.ee/public/bdoc_hashcode_example.zip

8.1.1.1.2 BDOC konteineri teisendamine tagasi standardkujule

Kui on tegemist päringuga mis **tagastab** konteineri, tuleb sooritada analoogsed teisendused vastupidises järjekorras:

1) Lisada andmefailid tagasi konteineri juurkataloogi (konteiner on sisemiselt ZIP-formaadis). Eraldi tasub tähelepanu pöörata järgmisele:

- Kõikidel konteineris olevatel failidel peab olema ka ZIP-faili kommentaar mis annab infot konteineri koostamisel kasutatud teegi kohta. Kommentaari sisu võib kopeerida lihtsalt teistelt ZIP-failis olevatelt failidelt (näiteks „mimetype“-faililt). Allkirja failidel (signatureN.xml) on soovitatav säilitada algses konteineris olnud kommentaar. Kommentaari näide:
  ```
  LIB DigiDocService/3.6.4 format: BDOC/2.1 Java:
  1.7.0_51/Oracle Corporation OS: Windows 8/amd64/6.2
  JVM: Java HotSpot(TM) 64-Bit Server VM/Oracle
  Corporation/24.51-b03
  ```

- Juurkataloogis olev “mimetype"-fail peab jääma pakkimata kujule (viimane on vajalik ühilduvuse tagamiseks väljaspool Eestit kasutatava tarkvaraga); samuti peab fail jääma ZIP-arhiivis esimeseks failiks.

2) Kustutada `META-INF` kataloogist räsifailid nimedega `hashcodes-*.xml`.

Peale taolisi teisendusi on BDOC konteiner taas tavakujul ja seega ka kasutatav näiteks DigiDoc3 klient tarkavaraga:

```
├── META-INF
│   ├── manifest.xml
│   └── signatures0.xml
├── file1.txt
├── File2.docx
└── mimetype
```

8.1.1.2 DigiDoc (DDOC) vorming ja HASHCODE

Variant 1 – Andmefaili asemel räsikoodi saatmine allkirjastamiseks

Olgu soov digitaalallkirjastada 42-baidine (sh 2 CRLF reavahetust) tekstifail test.txt, järgmise sisuga:

This is a test file
secondline
thirdline

Koostame järgmise, **kanoniseeritud**[1] kujul, XML-elemendi, kus väärtus „VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsaW5l“ on andmefaili sisu Base64 kujul ning lõpumärgendi </DataFile> ette lisatakse reavahetus:

[1] Kanoniseeritud XML-i kohta loe siit: http://www.w3.org/TR/xml-c14n

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

Eeldusel, et XML-is on kanoniseerimise tõttu reavahetused CRLF (\r\n) asendatud reavahetustega LF (\n), andmefail on Base64 kujul 64-sümboli pikkuste ridadena ning DataFile elemendi väärtused (sh atribuutide väärtused) on UTF8 kodeeringus, arvutame SHA-1 räsi üle kogu DataFile XML-elemendi, tulemuseks saame HEX-kujul stringi „b7c7914ab293811e0f0002932d85860a3b934890“ – selle konverteerime binary-stringiks ehk järjestikuste baitide jadaks: 0xb7, 0xc7, 0x91, ..., 0x90, mille viime Base64 kujule ja saame väärtuse „t8eRSrKTgR4PAAKTLYWGCjuTSJA=“.

PHP-s käiks viimase väärtuse saamine järgmiselt:
base64_encode(pack("H*", "b7c7914ab293811e0f0002932d85860a3b934890"));

Koostame StartSession Datafile parameetri täitmiseks andmestruktuuri (olgu nimega $inputData) järgmiste väärtustega:

Filename=“test.txt“
MimeType=“text/plain“
ContentType=“HASHCODE“
Size=42
DigestType=“sha1“
DigestValue=“t8eRSrKTgR4PAAKTLYWGCjuTSJA=“

Saadame StartSession meetodiga andmestruktuuri teenusele:

StartSession(„“, „“, TRUE, $inputData);

Järgnevalt sooritatakse teenuse vastu toiminguid allkirjastatavate failide täiendavaks lisamiseks (vt. meetodit AddDataFile), digitaalallkirja lisamiseks jne. Lõpuks küsitakse digitaalallkirjastatud konteiner teenuselt meetodiga GetSignedDoc.

Saadud konteineris tuleb XML element <DataFile ... ContentType="HASHCODE" ... Id="D0" ... > ... </DataFile> asendada eelnevalt koostatud xml elemendiga:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

Nüüd peaks olema valmis digidoc formaadile vastav konteiner.

Variant 2 – konteineri saatmine teenusesse nii, et andmefail on asendatud räsikoodiga

Näiteks kui DigiDoc konteineris on DataFile blokk kujul:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

ja teenusele ei soovita andmefaili sisu saata, tuleks blokk asendada alljärgnevaga:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="HASHCODE" Filename="test.txt" Id="D0" MimeType="text/plain"
Size="42" DigestType="sha1"
DigestValue="t8eRSrKTgR4PAAKTLYWGCjuTSJA="></DataFile>

Kui teenusesse on saadetud andmefailide sisu asemel räsi, tuleb teenusest (näiteks peale konteineri verifitseerimist või allkirjade lisamist) DigiDoc faili tagasi saamisel andmefaili sisaldav <DataFile> element tagasi asendada. Vastasel juhul ei ole tegemist korrektse DigiDoc vormingus failiga.

8.2 CloseSession

CloseSessioni päringuga lõpetatakse transaktsioon. Päringu tulemusena kustutatakse kogu antud sessioonijooksul serverisse talletatud info. Pärast CloseSession päringu kasutamist tuleb uue sessiooni algatamiseks teha uuesti StartSession päring. Alati on soovitatav transaktsioon CloseSession päringuga lõpetada. Kui rakendus sessiooni ise ei lõpeta, siis lõpetatakse sessioon automaatselt timeout´i saabumisel.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	kui sessiooni sulgemine õnnestub, on antud parameetri väärtuseks OK.

Kui sessiooni sulgemine mingil põhjusel ebaõnnestub tagastatakse SOAP-FAULT objekt.

8.3 CreateSignedDoc

CreateSignedDoc päringut kasutatakse uue DigiDoc konteineri loomiseks juhul, kui rakendus soovib määrata moodustatava konteineri formaati ja versiooni. CreateSignedDoc päringu moodustamise järgselt tuleb lisada AddDataFile päringuga andmed ja seejärel on võimalik fail allkirjastada.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	**aktiivse sessiooni identifikaator**
Format	String	+	loodava dokumendikonteineri formaat (hetkel toetatud DIGIDOC-XML 1.3 ja BDOC 2.1)
Version	String	+	loodava dokumendikonteineri formaadi versiooninumber. NB! Toetatud on DIGIDOC-XML 1.3 ja BDOC 2.1

NB! Toetatud on konteineri formaadid DIGIDOC-XML 1.3 ja BDOC 2.1. Kui päringu parameetrites kasutatakse mittetoetatud dokumendikonteineri formaati, siis tagastatakse SOAP veaobjekt veateatega "**Invalid format and version combination!**".

Digitaalallkirjade formaatide kirjeldused leiab http://www.id.ee/index.php?id=36103

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	toimingu vastuskood, kui toiming õnnestus on vastuskood "OK".
SignedDocInfo	String	Sessioonis oleva DigiDoc konteineri struktuur andmefaili lisamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

8.4 AddDataFile

AddDataFile päring võimaldab sessioonis olevale DigiDoc konteinerile lisada täiendava algfaili. Kui StartSession käigus on lisatud üks andmefail, kuid kasutaja soovib ühe DigiDoc konteineri sees allkirjastada mitut andmefaili, siis saab antud meetodiga enne allkirjastamist lisada ülejäänud algfailid. Andmefailidele kehtib mahupiirang 4 MB. Suuremaid faile saab DigiDocService-ile saata HASHCODE kujul, vt. selgitus allpool.

NB! Andmefaili lisamine on võimalik ainult nende DigiDoc failide puhul, millele ei ole lisatud ühtegi allkirja.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator.
Filename	String	+	andmefaili nimi ilma teekonnata.
MimeType	String	+	algandmete andmetüüp.

ContentType	String	+	Andmefaili sisu tüüp (HASHCODE, EMBEDDED_BASE64) **HASHCODE** – teenusele ei saadeta tervet andmefaili sisu, vaid ainult üle andmete arvutatud räsikood. Räsikoodi arvutamise algoritm on määratud parameetris *DigestType* ja räsikood edastatakse parameetrina *DigestValue.* Vaata näidist, kuidas algandmefailist räsi arvutada ning teenusele saata punktist 8.1. **EMBEDDED_BASE64 –** Faili sisu on esitatud Base64 kujul Content parameetris.
Size	Integer	+	tegeliku algandmefaili suurus baitides
DigestType	String	-	algandmefaili räsikoodi tüüp. DIGIDOC-XML formaadi korral on toetatud "sha1", BDOC formaadi korral "sha256". Nõutud vaid HASHCODE tüüpi faili puhul.
DigestValue	String	-	algandmefaili räsikoodi väärtus Base64 kujul. Nõutud vaid HASHCODE tüüpi faili puhul. DIGIDOC-XML formaadi korral arvutatakse räsi üle vastava DigiDoc <Datafile> elemendi kanoniseeritud kuju (räsi arvutamise kohta vaata punktist 8.1). BDOC formaadi korral arvutatakse räsi üle binaarse andmefaili.
Attributes	String	-	Suvaline hulk muid atribuute (metaandmed), mis lisatakse DigiDoc faili koosseisu <Datafile> plokki atribuutideks kujul <nimi>="<väärtus>".
Content	String	-	andmefaili sisu Base64 kujul, täidetakse vaid EMBEDDED_BASE64 ContentType korral

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	toimingu vastuskood, kui toiming õnnestus on vastuskood “OK”.
SignedDocInfo	SignedDocInfo	Sessioonis oleva DigiDoc konteineri struktuur andmefaili lisamise järgselt. SignedDocInfo struktuur on kirjeldatud peatükis 9.1.

8.5 MobileSign

MobileSign meetod käivitab sessioonis oleva DigiDoc faili allkirjastamise Mobiil-ID’ga.

MobileSign meetodi kasutamiseks peab sessioonis olevale DigiDoc konteineris olema vähemalt üks andmefail.

Kui soovitakse mobiiliga allkirja anda ilma DigiDoc faili loomata või teenusesse saatmata, tuleks kasutada antud meetodi asemel MobileCreateSignature meetodit.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignerIDCode	String	+	Allkirjastaja isikukood; Kohustuslik on kas SignerIDCode või SignerPhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud SignerIDCode ja SignerPhoneNo.
SignersCountry	String	-	Isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE);
SignerPhoneNo	String	+	allkirjastava isiku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301. Kohustuslik on kas SignerIDCode või SignerPhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud SignerIDCode ja SignerPhoneNo (vt. peatükk 5.2). Kui element “ SignerPhoneNo ” on määratud, siis teenuse siseselt lähtutakse prefiksis määratud riigi tunnusest (sõltumata elemendi "SignersCountry " väärtusest)
ServiceName	String	+	Teenuse kasutaja ja pakkuja vahel eelnevalt kokku lepitud teenuse nimetus. Maksimaalne pikkus 20 tähemärki.
AdditionalDataToBeDisplayed	String	-	Allkirjastamise käigus telefonil kuvatav lisatekst. Maksimaalne pikkus 40 baiti (ladina tähtede puhul tähendab see ühtlasi ka 40 sümboli pikkust teksti, aga näiteks kirillitsa teksti puhul võidakse tähti kodeerida 2 baidistena ja siis ei saa saata pikemat kui 20-sümbolilist teksti).
Language	String	+	Allkirjastaja telefonile kuvatavate teadete keel. Kasutatakse ISO 639: 3-tähelisi koode suurtähtedes. Variandid: EST, ENG, RUS, LIT.
Role	String	-	Allkirjastaja sisestatud rolli või resolutsioon.
City	String	-	Allkirjastamise asukoha linna nimi.
StateOrProvince	String	-	Allkirjastamise asukoha maakonna nimi.
PostalCode	String	-	Allkirjastamise asukoha postiindeks.
CountryName	String	-	Allkirjastamise asukoha riiginimi.
SigningProfile	String	-	- „**LT_TM**“ (ingl k *Long Term with Time Mark)*: Tähistab allkirjastamisprofiili BDOC-TM (BDOC allkiri koos ajamärgendiga) ja DDOC-vormingute jaoks. “LT_TM” on praeguses teenuse versioonis vaikeväärtus, st. kui parameeter on väärtustamata, siis loetakse selle väärtuseks “LT_TM”.

			- „**LT**“ (ingl k *Long Term*). Kasutatakse standardsete ajatemplitega BDOC-TS (ASiC-E) allkirjade loomiseks. Hetkel on tegemist reserveeritud väärtusega mis tagastab veakoodi 101 ja ja veateate “"BDOC-TS signature format is not supported in the current service version. For signing BDOC files with Mobile-ID, please use BDOC-TM format" . Antud meetodile “LT” profiili kasutamise tugi on plaanis lisada teenuse versioonis 3.9.
MessagingMode	String	+	Määrab mis režiimis tagastatakse MobileSign päringu vastus. Võimalikud variandid on: - “asynchClientServer” – Rakenduse pakkuja teeb pärast MobileSign päringut täiendavaid staatusepäringuid. - “asynchServerServer” – Signeerimistoimingu lõppemisel või vea tekkimisel saadetakse vastus kliendirakendusele asünkroonselt vastavalt AsyncConfiguration parameetris määratud konfiguratsioonile
AsyncConfiguration	Integer	-	Määrab asünkroonselt vastuse tagasisaatmiseks kasutatava konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul kui MessagingMode on “asynchServerServer”. Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel.
ReturnDocInfo	Boolean	+	kui väärtus “true”, tagastatakse päringu tulemusena DigiDoc faili info.
ReturnDocData	Boolean	+	**“**true” väärtuse korral tagastatakse DigiDoc dokument HTMLescaped kujul

Päringu vastus:

Välja nimetus	**Tüüp**	**Kirjeldus**
Status	String	väärtus „OK“ või veastring.
StatusCode	String	0 kui toiming õnnestus, vastasel korral veakood
ChallengeID	String	4 numbriline kontrollkood, mis arvutatakse signeeritava räsi põhjal. Antud kontrollkood tuleb mobiilallkirjastamist võimaldaval rakendusel kuvada kasutajale ja selle kaudu on võimalik kasutajal veenduda päringu autentsuses (sama kontrollkoodi kuvab ka telefon PIN2 küsimisel).

Kui kasutatakse asynchClientServer režiimi tuleb pärast antud päringu vastuse saamist hakata teenusele saatma GetStatusInfo päringuid veendumaks, et allkirjastamine on lõpule jõudnud.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 10 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda. Mobiil-ID toimingud aeguvad hiljemalt 4 minuti jooksul.

Juhul, kui kasutatakse "asynchServerServer" režiimi saadetakse allkirjastamise toimingu lõppemisel automaatselt teenuse kasutajale vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel "OK". Teised võimalikud olekud on kirjeldatud GetSignedDocInfo päringu vastuses Status väljal.
Data	String	a) Kui mobiilallkirjastamise päringu käivitanud meetodis oli ReturnDocInfo elemendi väärtus "true", siis on antud parameetri väärtuseks sessioonis oleva allkirjastatud faili struktuur XML-ina vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul b) Kui mobiilallkirjastamise päringu käivitanud meetodis oli ReturnDocInfo väärtus "false" ja ReturnDocData elemendi väärtuseks "true", siis on antud parameetri väärtuseks sessioonis olev DigiDoc fail HTML encoded kujul. c) Kui päringus on nii ReturnDocInfo kui ReturnDocData väärtused "false" on antud parameetri väärtus tühi.

8.6 GetStatusInfo

GetStatusInfo meetod on mõeldud teenusest sessiooni olekuinfo saamiseks.

GetStatusInfo päringut kasutatakse peamiselt mobiilallkirjastamise puhul asünkroonses Client-Server režiimis allkirjastamise protsessi olekuinfo pärimiseks (pollimiseks).

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	Aktiivse sessiooni identifikaator
ReturnDocInfo	Boolean	+	"true" väärtuse korral tagastatakse vastuses sessioonis oleva dokumendi info SignedDocInfo plokis.
WaitSignature	Boolean	+	Kui TRUE, siis päringule enne vastust ei tagastata kui telefonilt on signatuuri väärtus saabunud või on juhtunud viga. FALSE korral tagastatakse koheselt vastus ja GetStatusInfo väljakutset tuleb natukese aja pärast (2-10 sekundit) korrata.

Päringu vastus:

Parameeter	Tüüp	Kirjeldus
StatusCode	String	Viimase toimingu staatuse kood. Mobiilallkirjastamise puhul: - REQUEST_OK – sõnum täitmiseks vastu võetud; - EXPIRED_TRANSACTION – tegevus aegus, enne kui kasutaja jõudis allkirjastada; - USER_CANCEL - kasutaja katkestas telefonil allkirjastmise; - SIGNATURE - allkirjastamine edukalt lõpetatud; - NOT_VALID - tekkinud signatuur ei valideeru; - OUTSTANDING_TRANSACTION – toiming kestab, staatuse päringut tuleb korrata; - MID_NOT_READY - telefoni Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti; - PHONE_ABSENT – sõnumi saatmine ebaõnnestus, telefon ei ole levis; - SENDING_ERROR – muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - REVOKED_CERTIFICATE – Tühistatud sertifikaat - INTERNAL_ERROR – muu tehniline viga.
Status	String	Viimasena välja kutsutud toimingu olekukood. Päringu õnnestumisel „OK“ või veastring.
SignedDocInfo	SignedDocInfo	Juhul, kui GetStatusInfo päringus oli parameetri ReturnDocInfo väärtus “true”, tagastatakse sessioonis oleva allkirjastatud faili struktuur vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul.

8.7 GetSignedDocInfo

GetSignedDocInfo päring on mõeldud teenusest hetkel sessioonis oleva (allkirjastatud) dokumendi ja selle olekuinfo saamiseks.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator

Päringu vastusena tagastatav info:

Välja nimetus	Tüüp	Kirjeldus
Status	String	väärtus „OK“ või veastring
SignedDocInfo	SignedDocInfo	sessioonis oleva allkirjastatud faili struktuur vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul.

8.8 GetSignedDoc

GetSignedDoc päringuga saadakse veebiteenusest tagasi allkirjastatud dokument. Dokumenti sisu on HTML-encoded kujul. Kui lisaks allkirjastatud dokumendile soovitakse saada struktureeritud kujul dokumendi infot, tuleb kasutada GetSignedDocInfo päringut.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	väärtus „OK“ või veastring
SignedDocData	String	Sessioonis oleva allkirjastatud dokument XML kujul. Kuna XML märgised on viidud HTMLencoded kujule, siis tuleks enne faili salvestamist failisüsteemi või andmebaasi teha HTML decode teisendus.

8.9 GetDataFile

GetDataFile päring on allkirjastatud failist algfaili pärimiseks. Näiteks kui laadida StartSession päringuga teenusesse allkirjastatud fail, siis GetDataFile päringuga on võimalik kõik algfailid ükshaaval välja lugeda.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
DataFileId	String	+	andmefaili identifikaator. Kujul Dxx, kus xx on faili järjenumber. Sessioonis oleva allkirjastatud failis sisalduvate algfailide identifikaatorid on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
DataFileData	DataFileInfo	Algandmefaili info DataFileInfo stuktuurina, mis on kirjeldatud käesolevas dokumendis peatükis 9.3. Andmefailid tagastatakse samal kujul, nagu nad teenusele StartSession või AddDataFile meetoditega edastati, st. kui teenusele saadeti andmefaili sisu, siis

		antud meetod tagastab ka andmefaili bloki nii, et DfData väljal on andefaili sisu Base64 kujul. Juhul, kui teenusele edastati vaid andmefaili räsi, siis tagastab ka antud meetod andmefaili kohta vaid räsi.

Kui proovitakse pärida andmefaili, mida ei eksisteeri, tagastatakse SOAP-i vea objekt veateatega "**No such DataFile!**".

8.10 RemoveDataFile

RemoveDataFile päring võimaldab DigiDoc konteinerist eemaldada algfaili. NB! andmefaili eemaldamine on võimalik vaid siis kui konteiner ei sisalda mitte ühtegi allkirja. Kui dokumendile on lisatud üks või rohkem allkirja, siis andmefaili eemaldamine võimalik ei ole.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
DataFileId	String	+	andmefaili identifikaator. Kujul Dxx, kus xx on faili järjenumber. Sessioonis oleva allkirjastatud failis sisalduvate algfailide identifikaatorid on kättesaadavad *SignedDocInfo* struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks *StartSession* või *GetSignedDocInfo* päringu tulemusena.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK" või veastring
SignedDocInfo	SignedDocInfo	Sessioonis oleva DigiDoc-i info algfaili eemaldamise järgselt. SignedDocInfo struktuur on kirjeldatud peatükis 9.1.

Juhul, kui andmefaili eemaldamine ei õnnestu tagastatakse SOAP veaobjekt. Näiteks kui proovitakse eemaldada faili allkirjastatud dokumendilt, tagastatakse viga "Cannot change a signed doc".

8.11 RemoveSignature

RemovesSignature päring võimaldab Sessioonis olevalt allkirjastatud faililt eemaldada allkirja. Päringu tulemusena tagastatakse SignedDocInfo eemaldatud allkirjaga kujul.

Päring:

Parameeter	Tüüp	K	Kirjeldus

Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignatureId	String	+	allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
SignedDocInfo	SignedDocInfo	Sessioonis oleva DigiDoc-i info allkirja eemaldamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

Juhul, kui allkirja eemaldamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature id**! – allkirja identifikaator on määramata
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud

8.12 GetSignersCertificate

Allkirjastaja sertifikaadi päring. Päring võimaldab soovi korral (näiteks kasutajale kuvamiseks) teenuse kasutajal lugeda DigiDoc failist välja allkirjastaja sertifikaadi.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignatureId	String	+	allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring

CertificateData	String	päritud sertifikaat stringina Base64 kujul (PEM formaadis)

Juhul, kui sertifikaadi tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.

8.13 GetNotarysCertificate

Päringu tulemusena tagastatakse määratud allkirja kehtivuskinnituse allkirjastaja sertifikaat (OCSP serveri sertifikaat).

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignatureId	String	+	allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
CertificateData	String	päritud sertifikaat stringina Base64 kujul (PEM formaadis)

Juhul, kui sertifikaadi tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.
- **No notary for this Signature**! – päringu parameetriks oleval allkirjal ei ole kehtivuskinnitust.

8.14 GetNotary

Antud päring võimaldab teenuselt saada määratud allkirja kehtivuskinnitus.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignatureId	String	+	allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
OcspData	String	OCSP kehtivuskinnitus Base64 kujul

Juhul, kui kehtivuskinnituse hankimine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated**:**

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.
- **No notary for this Signature!** – päringu parameetriks oleval allkirjal ei ole kehtivuskinnitust.

8.15 GetVersion

Päring võimaldab kontrollida teenuse töötamist ja saada teada teenuse versiooni. Päringul parameetrid puuduvad.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Name	String	teenuse nimetus (hetkel DigiDocService)
Version	String	teenuse versioon kujul x.x.x (näiteks 1.0.3) Versiooni kõige suurem järk märgib põhjalikke muudatusi teenuses, versiooni numbri teine järk kirjeldab muudatusi, mille tulemusena võib muutuda teenuse protokoll ja viimane järk kirjeldab pisiparandusi, mis protokolli ei muuda.
Libname	String	kasutatava baasteegi nimetus
Libver	String	kasutava baasteegi versioon

8.16 PrepareSignature

Päring kiipkaardiga allkirjastamise korral allkirja ettevalmistamiseks. Päringu tulemusena lisatakse sessioonis olevale DigiDoc konteinerile uus nö. poolik allkiri ning tagastatakse uue allkirja unikaalne tunnus ja allkirjastatav räsikood, mis tuleks teenust kasutava rakenduse poolt edastada kasutaja arvutis olevale allkirjastamismoodulile, mis käivitatakse kasutaja brauseris.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignersCertificate	String	+	allkirjasta sertifikaat binaarselt kujult (DER) viiduna HEX stringi kujule. Enamasti sertifikaat antakse õigel kujul kasutaja arvutis oleva signeerimisprogrammi (allkirjastamismooduli) poolt
SignersTokenId	String	+	kiipkaardil privaatvõtme pesa identifikaator, väärtus määratakse signeerimisprogrammi poolt allkirjastaja sertifikaadi väljalugemisel ja edastatakse signeerimisprogrammile signeerimistoimingu teostamisel.
Role	String	-	Allkirjastaja poolt sisestatud rolli või resolutsiooni tekst
City	String	-	Allkirjastamise asukoha linna nimi
State	String	-	Allkirjastamise asukoha maakonna nimi
PostalCode	String	-	Allkirjastamise asukoha postiindeks
Country	String	-	Allkirjastamise asukoha riiginimi
SigningProfile	String	-	- „**LT_TM**“ (ingl k *Long Term with Time Mark)*: Tähistab allkirjastamisprofiili BDOC-TM (BDOC allkiri koos ajamärgendiga) ja DDOC-vormingute jaoks. “LT_TM” on praeguses teenuse versioonis vaikeväärtus, st. kui parameeter on väärtustamata, siis loetakse selle väärtuseks “LT_TM”. - „**LT**“ (ingl k *Long Term*). Kasutatakse standardsete ajatemplitega BDOC-TS (ASiC-E) allkirjade loomiseks. Hetkel on tegemist reserveeritud väärtusega mis tagastab veakoodi 101 ja ja veateate “"BDOC-TS signature format is not supported in the current service version. For signing BDOC files with Mobile-ID, please use BDOC-TM format" . Antud meetodile “LT” profiili kasutamise tugi on plaanis lisada teenuse versioonis 3.9.

Allkirjastamise asukohainfo küsib enamasti allkirjastamisrakendus kasutajalt ning edastav DigiDocServicele. Rolli ja allkirjastamise asukoha info sisestamine ei ole kohustuslik.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
SignatureId	String	uue loodava allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Antud tunnust kasutades on võimalik hiljem allkiri kustutada või pärida allkirja atribuute (allkirjastaja sertifikaat, kehtivuskinnituse sertifikaat, kehtivuskinnitus).
SignedInfoDigest	String	Allkirjastatav räsikood HEX string kujul

Juhul, kui kehtivuskinnituse tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature certificate! –** allkirjastaja sertifikaadi väärtus on tühi.

8.17 FinalizeSignature

Antud päring on allkirjastamise lõpetamiseks kiipkaardiga allkirjastamise korral. FinalizeSignature päringuga lõpetatakse PrepareSignature sammul ettevalmistatud allkiri. DigiDoc faili lisatakse allkirjastatud signatuur ja võetakse OCSP kehtivuskinnitus.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	aktiivse sessiooni identifikaator
SignatureId	String	+	allkirja unikaalne tunnus. Allkirja identifikaator tagastati teenuse poolt PrepareSignature sammu tulemusena.
SignatureValue	String	+	Signatuuri (allkirjastatud räsi) väärtus HEX stringi kujul. Antud väärtus tagastatakse signeerimiseks kasutatud brauseri mooduli poolt.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Status	String	päringu õnnestumise korral „OK“ või veastring
SignedDocInfo	SignedDocInfo	Sessioonis oleva DigiDoc-i info uue allkirja lisamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

8.18 MobileCreateSignature

Meetod Mobiil-ID-ga allkirjastamise protsessi käivitamiseks.

Meetodi kasutamise tulemusena tagastatakse DigiDoc-i <Signature> element ja teenust väljakutsuv rakendus peab ise hoolitsema selle lisamise eest DigiDoc faili koosseisu.

Meetod hoolitseb sisemiselt allkirjastaja sertifikaadi, kehtivuskinnituse ja vajadusel RFC3161 ajatemplite hankimise ning signeerimispäringu kasutaja telefonile saatmise eest.

Päringu kasutamiseks ei ole vaja luua StartSession meetodiga uut sessiooni. Kui soovitakse allkirjastada sessioonis olevat DigiDoc faili, tuleb antud meetodi asemel kasutada MobileSign meetodit.

NB! Toetatud on DIGIDOC-XML 1.3 ja BDOC 2.1. Kui päringu parameetrites kasutatakse mittetoetatud dokumendikonteineri formaati, siis tagastatakse SOAP veaobjekt veateatega "**Invalid format and version combination!**"

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Allkirjastava isiku isikukood. Kohustuslik on kas IDCode või PhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud IDCode ja PhoneNo.
SignersCountry	String(2)	-	Allkirjastaja isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE).
PhoneNo	String	+	Allkirjastaja telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301. Kohustuslik on kas IDCode või PhoneNo, soovitatav on kasutada mõlemat sisendparameetrit! Leedu Mobiil-ID kasutajate puhul on kohustuslikud IDCode ja PhoneNo (vt peatükk 5.2). Kui element "PhoneNo" on määratud, siis teenuse siseselt lähtutakse prefiksis määratud riigi tunnusest (sõltumata elemendi "SignersCountry" väärtusest)
Language	String(3)	+	Kasutaja telefonil kuvatavate teadete keel. Kasutatakse 3-tähelisi koode suurtähtedes. Võimalikud variandid: EST, ENG, RUS ja LIT.
ServiceName	String(20)	+	Allkirjastamisel telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki. Eelnevalt on vajalik kasutatava teenuse nimetuse kokkuleppimine teenuse pakkujaga.
MessageToDisplay	String(40 baiti)	-	Täiendav tekst, mis allkirjastamise PIN-i küsimise eelselt lisaks teenuse nimetuse kasutaja telefonile kuvatakse. Maksimaalne pikkus 40 baiti (ladina tähtede puhul tähendab see ühtlasi ka 40 sümboli pikkust teksti, aga näiteks kirillitsa teksti puhul võidakse tähti kodeerida 2 baidistena ja siis ei saa saata pikemat kui 20-sümbolilist teksti).

<table>
<tr><td>Role</td><td>String</td><td>-</td><td>Allkirjastaja poolt allkirjastamisel sisestatud rolli või resolutsiooni tekst</td></tr>
<tr><td>City</td><td>String</td><td>-</td><td>Allkirjastamise asukoha linna nimi</td></tr>
<tr><td>StateOrProvince</td><td>String</td><td>-</td><td>Allkirjastamise asukoha maakonna nimi</td></tr>
<tr><td>PostalCode</td><td>String</td><td>-</td><td>Allkirjastamise asukoha postiindeks</td></tr>
<tr><td>CountryName</td><td>String</td><td>-</td><td>Allkirjastamise asukoha riiginimi</td></tr>
<tr><td>SigningProfile</td><td>String</td><td>-</td><td>- „LT_TM“ (ingl k Long Term with Time Mark): Tähistab allkirjastamisprofiili BDOC-TM (BDOC allkiri koos ajamärgendiga) ja DDOC-vormingute jaoks. “LT_TM” on praeguses teenuse versioonis vaikeväärtus, st. kui parameeter on väärtustamata, siis loetakse selle väärtuseks “LT_TM”.
- „LT“ (ingl k Long Term). Kasutatakse standardsete ajatemplitega BDOC-TS (ASiC-E) allkirjade loomiseks; väärtus toimib BDOC-failiformaadi puhul.</td></tr>
<tr><td>Datafiles</td><td>List</td><td>+</td><td>Andmefailide list (koosneb DataFileDigest elementidest)
Iga DataFileDigest elemendil on järgmised atribuudid:
<table>
<tr><th>Atribuut</th><th>K</th><th>Kirjeldus</th></tr>
<tr><td>Id</td><td>+</td><td>faili sisemine unikaalne tunnus. DIGIDOC-XML formaadi korral algavad andmefailide tunnused sümboliga 'D', millele järgneb faili järjekorranumber. BDOC formaadi korral edastatakse failinimi, mis peab olema unikaalne</td></tr>
<tr><td>DigestType</td><td>+</td><td>algandmefaili räsikoodi tüüp. DIGIDOC-XML formaadi korral on toetatud “sha1”. BDOC failiformaadi puhul on soovitatav räsialgoritm “sha256”.</td></tr>
<tr><td>DigestValue</td><td>+</td><td>algandmefaili räsikoodi väärtus Base64 kujul. DIGIDOC-XML formaadi korral arvutatakse räsi üle vastava DigiDoc <Datafile> elemendi kanoniseeritud kuju (räsi arvutamise kohta vaata punktist 8.1). BDOC formaadi korral arvutatakse räsi üle binaarse andmefaili ja seejärel base64 kodeeritakse.</td></tr>
<tr><td>MimeType</td><td>-</td><td>MimeType parafaili andmetüüp BDOC formaadi korral vaikimisi kasutatav Mime-Type on</td></tr>
</table></td></tr>
</table>

			"application/octet-stream". NB! BDOC puhul on väga oluline, et BDOC konteineris manifest.xml failis oleks kasutusel sama MimeType
Format	String	+	Allkirjastatud faili formaat (toetatud on “DIGIDOC-XML” ja “BDOC”)
Version	String	+	Allkirjastatud faili formaadi versioon (DIGIDOC-XML puhul on toetaud versioon “1.3”, BDOC puhul versioon “2.1”)
SignatureID	String	+	Loodava allkirja identifikaator. Väljakutsuv rakendus peab kontrollima milline on suurim eelnev allkirja ID ja kasutama sellest ühe võrra suuremat väärtust. Näiteks kui viimane allkiri on identifikaatoriga “S2”, peaks antud parameetri väärtus olema “S3”. Kui dokumendil ei ole ühtegi allkirja, tuleks väärtusena kasutada “S0”.
MessagingMode		+	Määrab, mis režiimis tagastatakse MobileCreateSignature päringu vastus. Võimalikud variandid on: - “asynchClientServer” – rakenduse pakkuja teeb pärast MobileCreateSignature päringut täiendavaid staatusepäringuid; - “asynchServerServer” – signeerimistoimingu lõppemisel või vea tekkimisel saadetakse vastus teenuse kasutajale asünkroonselt.
AsyncConfiguration	Integer	-	Määrab asünkroonselt vastuse tagasisaatmiseks kasutatava konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul, kui MessagingMode on “asynchServerServer”. Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel. Hetkel on toetatud vastuse tagasi saatmine kasutades Java Message Services (JMS) liidest.

Päringu vastus:

Välja nimetus	**Tüüp**	**Kirjeldus**
Sesscode	Integer	Loodud sessiooni identifikaator
ChallengeID	String	4 tähemärgiline kontrollkood, mis arvutatakse signeerimiseks saadetava räsi põhjal. Antud kontrollkood tuleb mobiilallkirjastamist võimaldaval rakendusel kuvada kasutajale ning selle kaudu on võimalik kasutajal veenduda päringu autentsuses (sama kontrollkood kuvatakse allkirjastamisel ka telefonile).
Status	String	Toimingu edukal täitmisel “OK”. Juhul kui meetodi väljakutsel juhtub viga tagastatakse SOAP veaobjekt. SOAP veaobjektide kirjeldus ja veakoodid on toodud peatükis 9.4

Kui kasutatakse “asynchClientServer” režiimi tuleb pärast antud päringule positiivse vastuse saamise järgselt teenusele saata GetMobileCreateSignatureStatus päringuid.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 10 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda. Mobiil-ID toimingud aeguvad hiljemalt 4 minuti jooksul.

Juhul, kui kasutatakse “asynchServerServer” režiimi, saadetakse mobiilallkirjastamise toimingu lõppemisel automaatselt teenuse kasutajale allolev vastus vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel "SIGNATURE". Teised võimalikud olekud on kirjeldatud GetMobileCreateSignatureStatus meetodi vastuses.
Data	String	Mobiilallkirjastamise käigus tekkinud <Signature> blokk halja XML-ina.

8.19 GetMobileCreateSignatureStatus

Antud meetodit kasutatakse ClientServer režiimis mobiilallkirjastamise protsessi oleku teada saamiseks.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	Sessiooni identifikaator
WaitSignature	Boolean	+	Kui TRUE, siis päringule ei tagastata vastust enne, kui telefonilt on signatuuri väärtus saabunud või on juhtunud viga. FALSE korral tagastatakse kohe vastus ja teenuse kasutaja peab tegema mõne aja möödumisel (soovitavalt 2-10 sekundi pärast) korduva staatuse päringu.

Päringu vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Sessiooni identifikaator
Status	String	Mobiilallkirjastamise protsessi olek: - REQUEST_OK – käsklus vastu võetud; - EXPIRED_TRANSACTION – tegevus aegus, enne kui kasutaja jõudis allkirjastada; - USER_CANCEL - kasutaja keeldus allkirjastamast või katkestas; - SIGNATURE - allkirjastamine edukalt tehtud;

		- OUTSTANDING_TRANSACTION – toiming kestab, staatuse päringut tuleb korrata; - MID_NOT_READY - telefoni Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti; - PHONE_ABSENT – telefon ei ole levis; - SENDING_ERROR – muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - NOT_VALID - tekkinud signatuur ei valideeru - REVOKED_CERTIFICATE – Tühistatud sertifikaat - INTERNAL_ERROR – teenuse tehniline viga
Signature	String	Tekitatud DigiDoc-i <Signature> element Base64 kujul

Kui vastuses on Status väärtus ei ole OUTSTANDING_TRANSACTION, siis meetodi välja kutsumise järgselt sessioon suletakse.

8.20 GetMobileCertificate

Meetod Mobiil-ID teenuse olemasolu ja sertifikaatide info pärimiseks.

NB! Antud meetodi kasutamine on täiendavalt piiratud ja vajalik on tellida sellele eraldi IP aadressi põhine ligipääs.

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Sertifikaadiomaniku isikukood.
Country	String(2)	-	Isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE).
PhoneNo	String	+	Sertifikaadiomaniku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301. Kui element “PhoneNo” on määratud, siis teenuse siseselt lähtutakse prefiksis määratud riigi tunnusest (sõltumata elemendi "Country" väärtusest)
ReturnCertData	String	-	Väärtused: “auth” – autentimissertifikaadi päring, “sign” –allkirjastamissertifikaadi päring, “both” – mõlemad, “none” mitte kumbagi. Vaikeväärtuseks on “none”.

Päringu vastus:

Parameeter	Tüüp	Kirjeldus
AuthCertStatus	String	OK – isikutuvastuse sertifikaat on ajaliselt kehtiv, ei kajasta sertifikaadi tegelikku staatust;

		REVOKED – sertifikaat on aegunud Soovi korral saab sertifikaadi kehtivuskinnitus teenusepakkujal küsida OCSP teenuse käest (nt. meetodiga CheckCertificate()).
SignCertStatus	String	OK – allkirjastamise sertifikaat on ajaliselt kehtiv, ei kajasta sertifikaadi tegelikku staatust; REVOKED – sertifikaat on aegunud Soovi korral saab sertifikaadi kehtivuskinnitus teenusepakkujal küsida OCSP teenuse käest (nt. meetodiga CheckCertificate()).
AuthCertData	String	Isikutuvastuse sertifikaat PEM kujul
SignCertData	String	Allkirjastamise sertifikaat PEM kujul

Kui kasutaja ei ole Mobiil-ID klient, antakse SOAP fault vastavalt 9.4 toodule.

8.21 MobileSignHashRequest

Meetod Mobiil-ID-ga räsi allkirjastamise protsessi käivitamiseks. Antud meetod on mõeldud allkirjastamaks teisi formaate kui DDOC ja BDOC (nt. PDF, ADOC jne). BDOC ja DDOC formaatide korral soovitame kasutada MobileCreateSignature ja MobileSign teenuse meetodeid.

Kui allkirjastamise protsessi käigus on vajalik hankida allkirjastaja sertifikaat ja see lisada enne räsi allkirjastamist dokumendile, siis selleks on mõeldud teenuse meetod GetMobileCertificate.

Meetod hoolitseb sisemiselt allkirjastaja sertifikaadi, kehtivuskinnituse ning signeerimispäringu kasutaja telefonile saatmise eest. Päringu kasutamiseks ei ole vaja luua uut sessiooni.

Räsi allkirjastamise protsessi olekut kontrollitakse ClientServer režiimis GetMobileSignHashStatusV2 teenusega. NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 10 sekundit kuna allkirjastamisprotsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda. Mobiil-ID toimingud aeguvad hiljemalt 4 minuti jooksul.

Antud meetod on document-literal stiilis ja kättesaadav uuelt alamaadressilt /v2/?wsdl. Uue teenuse versiooni jaoks on kasutusel eraldi WSDL ning lisaks on täiendatud teenuse veateadete sõnumi formaati (vt. Peatükk 9.4)

NB! Antud meetodi kasutamine on täiendavalt piiratud ja vajalik on tellida sellele eraldi IP aadressi põhine ligipääs.

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String(20)	+	Sertifikaadiomaniku isikukood.

PhoneNo	String(20)	+	Sertifikaadiomaniku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301.
Language	String(3)	+	Kasutaja telefonil kuvatavate teadete keel. Kasutatakse ISO 3166 3-tähelisi koode suurtähtedes. Võimalikud variandid: EST, ENG, LIT ja RUS.
MessageToDisplay	String(40)	-	Täiendav tekst, mis allkirjastamise PIN-i küsimise eelselt lisaks teenuse nimetuse kasutaja telefonile kuvatakse. Maksimaalne pikkus 40 tähemärki.
ServiceName	String(20)	+	Allkirjastamisel telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki.
Hash	String(128)	+	Allkirjastatav räsi. 128 tähemärki. Edastatakse HEX stringina.
HashType	String(20)	+	Allkirjastatava räsi tüüp. Hetkel toetakse sha1, sha256 ja sha512 räsisid.

Päringu vastus:

Parameeter	Tüüp	Kirjeldus
Sesscode	String	Sessiooni identifikaator.
ChallengeID	String	– 4 (number) tähemärgiline kontrollkood, mis arvutatakse kasutaja telefonile signeerimiseks saadetava Challenge väärtuse põhjal. – 40 tähemärgiline HEX ehk allkirjastatav räsi Challenge. Kasutusel ainult Bite MSSP operaatori korral. Antud kontrollkood tuleb mobiilallkirjastamist võimaldaval rakendusel kuvada kasutajale ja selle kaudu on võimalik kasutajal veenduda päringu autentsuses. NB! Mobiil-ID allkirjastamise rakendus peab paluma kasutajal kontrollida rakenduses ja telefonil kuvatava kontrollkoodi kokkulangevust.
Status	String	Toimingu edukal täitmisel “OK”. Juhul kui meetodi väljakutsel juhtub viga tagastatakse SOAP veaobjekt.

Juhul, kui meetodi väljakutsel juhtub viga, tagastatakse SOAP veaobjekt vastavalt peatükis 9.4 toodud kirjeldusele.

8.22 GetMobileSignHashStatusRequest

Meetod Mobiil-ID-ga räsi allkirjastamise protsessi (MobileSignHash) oleku teada saamiseks. Meetodi täpne nimi teenuse poole pöördumisel on GetMobileSignHashStatusRequest().

Teenus tagastab räsi allkirjastamise sessiooni staatuse ja eduka allkirjastamise korral ka allkirjastatud räsi, allkirjastaja sertifikaadi info ning sertifikaadi kehtivusinfo.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	String(20)	+	Sessiooni identifikaator.
WaitSignature	Boolean	-	Kui "true", siis päringule ei tagastata vastust enne, kui telefonilt on signatuuri väärtus saabunud või on juhtunud viga. "false" korral tagastatakse kohe vastus ja teenuse kasutaja peab tegema mõne aja möödumisel (soovitavalt 2-10 sekundi pärast) korduva staatuse päringu.

Päringu vastus:

Parameeter	Tüüp	Kirjeldus
Sesscode	String	Sessiooni identifikaator.
Status	String	Mobiilautentimise protsessi olek: - OUTSTANDING_TRANSACTION – allkirjastamise toiming kestab, staatuse päringut tuleb korrata; - SIGNATURE - allkirjastamine edukalt tehtud; - NOT_VALID – toiming on lõppenud, kuid kasutaja poolt tekitatud signatuur ei ole kehtiv. - EXPIRED_TRANSACTION – sessioon aegus ennem kui kasutaja jõudis allkirjastamise lõpetada; - USER_CANCEL – kasutaja keeldus allkirjastamast või katkestas allkirjastamise; - MID_NOT_READY - Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti - PHONE_ABSENT – telefon ei ole levis; - SENDING_ERROR – Muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - INTERNAL_ERROR – teenuse tehniline viga või sertifikaadi staatus on UNKNOWN; - REVOKED_CERTIFICATE - sertifikaat on tühistatud/peatatud; - OCSP_UNAUTHORIZED teenust kasutaval kliendil puudub juurdepääs DigiDocService'i poolt kasutatavale OCSP kehtivuskinnitusteenusele.
Signature	String	Krüpteeritud räsi PKCS1 / PKCS13 konteineris. (Tagastatakse ainult juhul kui Status == "SIGNATURE").
RevocationData	String	Sertifikaadi kehtivusinfo (PEM-formaadis).
CertificateData	String	Sertifikaat PEM formaadis Base64 enkodeerituna.

Juhul, kui meetodi väljakutsel juhtub viga, tagastatakse SOAP veaobjekt vastavalt peatükis 9.4 toodud kirjeldusele.

9 Kasutatavad andmestruktuurid

9.1 SignedDocInfo

Esitab terviklikult allkirjastatud DigiDoc faili struktuuri

- **Format** – Allkirjastatud konteineri failiformaat (hetkel toetatud DIGIDOC-XML ja BDOC)
- **Version** - Allkirjastatud failiformaadi versioon (DIGIDOC-XML puhul versioonid 1.1, 1.2, 1.3; BDOC puhul versioon 2.1)
- **DataFileInfo –** Konteineris sisalduvate andmefailide info. Andmestruktuur on kirjeldatud käesolevas dokumendis peatükis 9.3. Ühe SignedDocInfo plokis võib olla DataFileInfo plokk esineda 0..n korda sõltuvalt andmefailide arvust.
- **SignatureInfo** – Sisaldab allkirjastatud failis olevate allkirjade infot. Antud blokki võib olla 0..n arv korda sõltuvalt allkirjade arvust. Sisaldab järgmisi atribuute:
    - **Id –** Allkirja antud dokumendi/transaktsiooni piires unikaalne allkirjaidentifikaator. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber.
    - **Status** – Allkirja olekuinfo. Kui antud atribuudi väärtuseks on **“OK”** on allkiri kehtiv. Kui allkiri ei kehti on antud elemendi väärtuseks **“Error”** ja täpsem veainfo on esitatud Error elemendis. Kui allkiri on kehtiv aga ei vasta täielikult konteineri spetsifikatsioonile, siis on antud elemendi väärtus „OK“ ja Error elemendis on täpsem kirjeldus DigiDoc teegi poolt antud hoiatuse kohta.
    - **Error** – Sisaldab allkirja kehtivuse kontrollil ilmnenud vea infot. Sisaldab järgmisi atribuute:
        - **code** – veakood
        - **category –** veakategooria, hetkel on 3 veakategooriat: TECHNICAL –tehniline probleem; USER - kasutaja poolt likvideeritav probleem; LIBRARY – DigiDoc teegi sisene viga. WARNING – Tegemist on DigiDoc teegi poolt antud hoiatusega. Allkiri on juriidiliselt kehtiv aga edasised muudatused konteineris ei ole toetatud. Loe täpsemat selgitust hoiatuste kohta peatükis 9.5 „Konteineri valideerimine“.
        - **description –** vea tekstiline kirjeldus inglise keeles.
    - **SigningTime** – allkirja andmise lokaalne (nt. allkirjasta arvuti, allkirjastamise veebiserveri) aeg vastavalt “The W3C note Date and Time Formats” [5] esitatud kujul. NB! See ei ole allkirja „ametlik“ aeg, allkirja andmise ametlik aeg on määratud käesoleva struktuuri *Confirmation-> ProducedAt* elemendis.
    - **SignerRole –** allkirjastaja poolt allkirjastamisel märgitud roll või resulolutsioon. Määratud järgmiste atribuutidega:
        - **Certified –** Määrab, kas roll on allkirjastaja poolt ise määratud või sertifitseerija poolt antud. Hetkel kasutatakse

ainult kasutajapoolt määratavaid rolle, mille puhul antud parameetri väärtus on 0.
    - **Role –** Rolli või resolutsiooni tekst
- **SignatureProductionPlace -** Allkirja atribuutide hulka kuuluv andmehulk, mis kirjeldab allkirjastamise kohta. Allkirja andmisel on antud bloki täitmine mittekohustuslik. Sisaldab järgmisi andmeid:
    - **City** – Allkirjastamise asukoha linna nimi
    - **StateOrProvince** – Allkirjastamise asukoha maakonna nimi
    - **PostalCode** – Allkirjastamise asukoha postiindeks
    - **CountryName** – Allkirjastamise asukoha riiginimi

- **Signer** – info allkirjastaja kohta, sisaldab järgmisi atribuute:
    - **CommonName** – Allkirjastaja nimi, võetakse allkirjastaja sertifikaadi Subject väljalt CN parameetrist.
    - **IDCode** – allkirjastaja isikukood, võetakse allkirjastaja sertifikaadi Subjecti Serial Number parameetrist.
    - **Certificate** allkirjastamiseks kasutatud sertifikaadi põhiinfo vastavalt käesolevas dokumendis peatükis 9.2 esitatud kujul.
- **Confirmation –** OCSP kehtivuskinnituse andmete blokk. Iga korrektne kehtiv allkiri sisaldab ühte kehtivuskinnituse plokki. Confirmation plokk sisaldab järgnevaid atribuute:
    - **ResponderID** – OCSP kehtivuskinnituse serveri eraldusnimi (OCSP Responder ID)
    - **ProducedAt** – Kehivuskinnituse võtmise aeg vastavalt "The W3C note Date and Time Formats" [5] esitatud kujul. (näiteks "2005.09.14T21:00:00Z"). NB! Antud aega loetakse digitaalallkirja andmise ajaks.
    - **Responder Certificate –** Kehtivuskinnituse teenuse serveri (OCSP) sertifikaat vastavalt käesolevas dokumendis peatükis 9.2 esitatud kujul.
- **Timestamps –** Info allkirjaga seotud RFC3161 ajatemplite kohta. Antud teenuse versioonis ei ole ajatemplite funktsionaalsus realiseeritud.
- **CRLInfo –** Info allkirjaga seotud tühisusnimekirja kohta. Antud teenuse versioonis ei ole tühisusnimekirjadega seotud funktsionaalsus veel realiseeritud.

Näidisandmete blokk:

```
<SignedDocInfo xsi:type="d:SignedDocInfo">
   <format xsi:type="xsd:string"></format>
   <version xsi:type="xsd:string"></version>
   <DataFileInfo xsi:type="d:DataFileInfo">
      <Id xsi:type="xsd:string"></Id>
      <Filename xsi:type="xsd:string"></Filename>
      <MimeType xsi:type="xsd:string"></MimeType>
      <ContentType xsi:type="xsd:string"></ContentType>
      <Size xsi:type="xsd:int">0</Size>
      <DigestType xsi:type="xsd:string"></DigestType>
      <DigestValue xsi:type="xsd:string"></DigestValue>
```

```
            <Attributes xsi:type="d:DataFileAttribute">
            <name xsi:type="xsd:string"></name>
            <value xsi:type="xsd:string"></value>
         </Attributes>
      </DataFileInfo>
   <SignatureInfo xsi:type="d:SignatureInfo">
      <Id xsi:type="xsd:string"></Id>
      <Status xsi:type="xsd:string"></Status>
      <Error xsi:type="d:Error">
         <code xsi:type="xsd:int">0</code>
         <category xsi:type="xsd:string"></category>
         <description xsi:type="xsd:string"></description>
      </Error>
      <SigningTime xsi:type="xsd:string"></SigningTime>
      <SignerRole xsi:type="d:SignerRole">
            <certified xsi:type="xsd:int">0</certified>
            <Role xsi:type="xsd:string"></Role>
      </SignerRole>
      <SignatureProductionPlace
si:type="d:SignatureProductionPlace">
         <City xsi:type="xsd:string"></City>
         <StateOrProvince
      xsi:type="xsd:string"></StateOrProvince>
         <PostalCode xsi:type="xsd:string"></PostalCode>
         <CountryName xsi:type="xsd:string"></CountryName>
      </SignatureProductionPlace>
      <Signer xsi:type="d:SignerInfo">
         <CommonName xsi:type="xsd:string"></CommonName>
         <IDCode xsi:type="xsd:string"></IDCode>
         <Certificate xsi:type="d:CertificateInfo">
            <Issuer xsi:type="xsd:string"></Issuer>
            <Subject xsi:type="xsd:string"></Subject>
            <ValidFrom xsi:type="xsd:string"></ValidFrom>
            <ValidTo xsi:type="xsd:string"></ValidTo>
            <IssuerSerial
            xsi:type="xsd:string"></IssuerSerial>
            <Policies xsi:type="d:CertificatePolicy">
               <OID xsi:type="xsd:string"></OID>
               <URL xsi:type="xsd:string"></URL>
               <Description
                  xsi:type="xsd:string"></Description>
            </Policies>
         </Certificate>
      </Signer>
      <Confirmation xsi:type="d:ConfirmationInfo">
         <ResponderID xsi:type="xsd:string"></ResponderID>
         <ProducedAt xsi:type="xsd:string"></ProducedAt>
         <ResponderCertificate xsi:type="d:CertificateInfo">
            <Issuer xsi:type="xsd:string"></Issuer>
            <Subject xsi:type="xsd:string"></Subject>
            <ValidFrom xsi:type="xsd:string"></ValidFrom>
            <ValidTo xsi:type="xsd:string"></ValidTo>
```

```
            <IssuerSerial
            xsi:type="xsd:string"></IssuerSerial>
            <Policies xsi:type="d:CertificatePolicy">
               <OID xsi:type="xsd:string"></OID>
               <URL xsi:type="xsd:string"></URL>
               <Description
                  xsi:type="xsd:string"></Description>
            </Policies>
         </ResponderCertificate>
      </Confirmation>
   </SignatureInfo>
</SignedDocInfo>
```

9.2 CertificateInfo

Sertifikaadi põhivälju sisaldav andmeblokk. Kasutatakse nii allkirjastaja sertifikaadi, kui ka kehtivuskinnituse sertifikaadi info edastamiseks.

Sisaldab järgmisi atribuute:

- **Issuer** – Sertifikaadi väljaandja eraldusnimi (distinguished name)
- **IssuerSerial** - Sertifikaadi seerianumber
- **Subject** – Sertifikaadi eraldusnimi (distinguished name)
- **ValidForm** – Sertifikaadi kehtivuse algusaeg vastavalt The W3C note Date and Time Formats *[5] esitatud kujul. (näiteks "*2005.09.14T21:00:00Z")
- **ValidTo** – Sertifikaadi kehtivuse lõppemise aeg vastavalt [5] esitatud kujul.
- **Policies** - Kinnituspõhimõtete plokk, seda võib esineda 0..n tükki
  - **OID** - Kinnituspõhimõtete unikaalne tunnus
  - **URL –** Viide kinnituspõhimõtetele (kasutatakse peamiselt asutuste digitaalkinnituste põhjal)
  - **Description –**Kinnituspõhimõtete lühikirjeldus

Näidisandmete blokk:

```
<Certificate xsi:type="d:CertificateInfo">
   <Issuer
xsi:type="xsd:string">/emailAddress=pki@sk.ee/C=EE/O=AS
Sertifitseerimiskeskus/OU=ESTEID/SN=1/CN=ESTEID-SK</Issuer>
   <Subject xsi:type="xsd:string">/C=EE/O=ESTEID/OU=digital
signature/CN=KESKEL,URMO,38002240232/SN=KESKEL/GN=URMO/seria
lNumber=38002240232</Subject>
   <ValidFrom
xsi:type="xsd:string">2005.03.18T22:00:00Z</ValidFrom>
   <ValidTo
xsi:type="xsd:string">2008.03.22T22:00:00Z</ValidTo>
   <IssuerSerial
xsi:type="xsd:string">1111128454</IssuerSerial>
   <Policies xsi:type="d:CertificatePolicy">
```

```
      <OID
      xsi:type="xsd:string">1.3.6.1.4.1.10015.1.1.1.1</OID>
      <URL xsi:type="xsd:string">http://www.sk.ee/cps/</URL>
      <Description xsi:type="xsd:string">none</Description>
   </Policies>
</Certificate>
```

9.3 DataFileInfo

Antud andmeblokk kirjeldab DigiDoc konteineri koosseisus oleva või selle koosseisu lisatava andmefaili andmeid. Antud blokis võib sisalduda andmefail Base64 kujul, kuid blokk võib sisaldada ka vaid andmefaili räsi* - sõltuvalt ContentType atribuudi väärtusest.

- **Id** – faili sisemine unikaalne tunnus. DIGIDOC-XML formaadi korral algavad andmefailide tunnused sümboliga 'D', millele järgneb faili järjekorranumber. BDOC formaadi korral on tunnuseks failinimi, mis peab olema unikaalne. Startsession päringu käigus antud atribuuti ei väärtustata ja edastatakse tühistring.
- **Filename** – andmefaili nimi ilma teekonnata.
- **ContentType** – Andmefaili sisu tüüp (HASHCODE, EMBEDDED_BASE64)
  - **HASHCODE** – teenusele ei saadeta tervet andmefaili sisu, vaid ainult üle andmete arvutatud räsikood*. Räsikoodi arvutamise algoritm on määratud atribuudis *DigestType* ja räsikoodi ennast hoitakse väljal *DigestValue.*
  - **EMBEDDED_BASE64 –** Faili sisu on Base64 kujul DfData alamelemendis.
- **MimeType** – algandmete andmetüüp.
- **Size** – tegeliku algandmefaili suurus baitides.
- **DigestType** - algandmefaili räsi algoritm. DIGIDOC-XML formaadi korral on toetatud “sha1”, BDOC formaadi korral on toetatud “sha256”. Nõutud vaid HASHCODE tüüpi faili puhul.
- **DigestValue** – algandmefaili räsikood* väärtus Base64 kujul. Nõutud vaid HASHCODE tüüpi faili puhul.
- **Attributes** - Suvaline hulk muid atribuute (metaandmed), mis lisatakse DigiDoc faili koosseisu <Datafile> plokki atribuutideks kujul <nimi>="<väärtus>".
- **DfData** - andmefaili sisu Base64 kujul.

* Vaata näidist, kuidas algandmefailist räsi arvutada ning teenusele saata punktist 8.1

9.4 SOAP veakoodid

SOAP veaobjekt <faultstring> sisaldab veakoodi ja <detail><message> selgitavat teksti inglise keeles.

Meetodite MobileSignHash ja GetMobileSignHashStatus vastustes on kasutusel uus veaobjekti struktuur. Element <faultstring> sisaldab veakoodi. Element <detail> alamelemendiks on <endpointError> tüüpi objekt mis sisaldab ühte

<message> elementi veateate selgitava sõnumiga ja nulli või enamat <reason> elementi vea täpsemate kirjeldustega (vt. veateadete näiteid peatüki lõpus).

Veakoodid on grupeeritud järgmiselt:

- 100-199 - teenust kasutava kliendi põhjustatud vead
- 200-299 - teenusesisesed vead
- 300-399 - lõppkasutaja ja tema telefoniga seotud vead.

Veakoodide tähendused:

Veakood	Tähendus
100	Teenuse üldine veasituatsioon.
101	Sisendparameetrid mittekorrektsel kujul.
102	Mõni kohustuslik sisendparameeter on määramata
103	Teenusepakkujal puudub ligipääs SK kehtivuskinnituse teenusele (OCSP vastus UNAUTHORIZED).
200	Teenuse üldine viga.
201	Kasutaja sertifikaat puudub või ei õnnestunud saada ühendust sertifikaadi hoidlaga.
202	Kasutaja sertifikaadi kehtivust ei ole võimalik kontrollida.
203	Teenuse sessioon on lukustatud teise SOAP päringu poolt.
300	Kasutajaga telefoniga seotud üldine viga.
301	Kasutajal pole Mobiil-ID lepingut.
302	Kasutaja sertifikaat ei kehti (OCSP vastus REVOKED).
303	Kasutajal pole Mobiil-ID aktiveeritud. Aktiveerimiseks tuleks minna aadressile https://www.sk.ee/aktiveerimine.
304	Sertifikaat on peatatud staatuses.
305	Sertifikaat on aegunud.
413	Sisendsõnum ületab lubatud mahupiirangut.
503	Teenuse üheaegsete päringute arv on ületatud.

Teenuse veateate näidis 1:

Esimese versiooni teenuse päringus oli telefoni numbri formaat vale või telefoni numbri riigikood ei ole toetatud riigikoodide nimekirjas.

```
<SOAP-ENV:Fault>
   <faultcode>SOAP-ENV:Client</faultcode>
   <faultstring xml:lang="en">102</faultstring>
   <detail>
      <message>User IDcode and Phone number are
mandatory</message>
   </detail>
</SOAP-ENV:Fault>
```

Teenuse veateate näidis 2:

Teise versiooni teenuse päringu valideerimisel leiti mitu viga.

- Päringu parameetrite järjekord on vale. Esimesena oodati parameetrit "IDCode“.
- Telefoni number ei vasta oodatud andmetüübile.

```
<SOAP-ENV:Fault>
   <faultcode>SOAP-ENV:Client</faultcode>
   <faultstring xml:lang="en">101</faultstring>
   <detail>
      <endpointError>
         <message>Request message validation
failed</message>
         <reason>cvc-complex-type.2.4.a: Invalid content was
found starting with element 'MessageToDisplay'. One of
'{IDCode}' is expected.</reason>
         <reason>cvc-minLength-valid: Value '' with length =
'0' is not facet-valid with respect to minLength '5' for
type 'PhoneNumberType'.</reason>
         <reason>cvc-type.3.1.3: The value '' of element
'PhoneNo' is not valid.</reason>
      </endpointError>
   </detail>
</SOAP-ENV:Fault>
```

9.5 Konteineri valideerimine

Kui DigiDocService sisendis saata juba olemasolev dokumendi konteiner, teostab teenus selle konteineri valideerimise. Alates jDigiDoc teegi versioonist 3.8 on konteineri valideerimises tehtud muudatus, mis lubab konteineris teatud tehnilisi vigu. Selliseid vigu käsitletakse hoiatustena.

Hoiatuse korral loetakse dokumendi konteiner ja selles sisalduvad allkirjad juriidiliselt kehtivaks. Teatud hoiatuste korral on edasised konteineri muudatused blokeeritud (allkirja eemaldamine / lisamine ei ole lubatud). Hoiatustena käsitletakse järgmisi jDigiDoc teegi veakoode:

- 129 WARN_WEAK_DIGEST - konteineris kasutatakse liiga nõrka räsi arvutamise algoritmi. Allkirja lisamine on blokeeritud.
- 173 ERR_DF_INV_HASH_GOOD_ALT_HASH - DataFile elemendil puudub nimeruumi atribuut. Allkirja lisamine on blokeeritud.
- 176 ERR_ISSUER_XMLNS - X509IssuerName või X509SerialNumber elemendil puudub nimeruumi atribuut.
- 177 ERR_OLD_VER - Dokumendi konteineri versioon ei ole enam toetatud. Allkirja lisamine on blokeeritud.

Täpsemalt ja detailsemalt saab lugeda jDigiDoc teegi dokumentatsioonist http://www.id.ee/public/SK-JDD-PRG-GUIDE.pdf ptk “Validation status VALID WITH WARNINGS”.

Teenuse väljundis on hoiatused näha ainult SignatureInfo elemendis. Hoiatuse korral on SignatureInfo alamelemendi Status väärtus OK aga ühtlasi on olemas ka Error element. Hoiatuse korral on Error elemendi alamelemendi category väärtuseks WARNING. Code ja description elemendid kirjeldavad täpsemat hoiatuse põhjust.

10 Teenuse muudatuste ajalugu

Teenuse muudatuste ajalugu on leitav http://www.id.ee/ddschangelog.